И. М. ВИНОГРАДОВ

МЕТОД ТРИГОНОМЕТРИЧЕСКИХ СУММ В ТЕОРИИ ЧИСЕЛ

數論中的三角和法

И. М. 維諾格拉朵夫

目　　錄

記　　號

θ 記絕對值不大於 1 的數；c 爲正常數；ε 爲任意小的正數.

當 $B>0$ 時,記號 $A\ll B$ 是指 $|A|\leqslant cB$.

設變量 S 的值所成的集合完全定義，任何 $\ll H$ 項之和,其每項皆屬於所說之集合者，以記號 $\sum^{H} S$ 記之.

對於滿足條件 $0<B-A<1$ 之實數 A 與 B,記號 $A<z<B \pmod 1$, $A\leqslant z<B \pmod 1$, $A<z\leqslant B \pmod 1$, $A\leqslant z\leqslant B \pmod 1$ 分別表示對於某整數 h,我們有

$$A+h<z<B+h;\quad A+h\leqslant z<B+h;\quad A+h<z\leqslant B+h;$$
$$A+h\leqslant z\leqslant B+h.$$

對於實數 x，記號 $\{x\}$ 表示 x 的分數部分,卽 $x-[x]$,而記號 (x) 則爲 x 到其最近整數的距離,卽 $\min(\{x\},1-\{x\})$.

記號 $\Omega(d)$ 是正數 d 的素因子的個數；n 是大於 1 的整常數；$\nu=\frac{1}{n}$.

所謂《整點》是指座標皆爲有理整數之點.

緒　論

數論裏最重要的問題之一，就是對於單元或多元函數 $f(x_1,\cdots,x_r)$ 之值的分佈建立各種規律．但此時祇考慮與 r 次元空間中，屬於所與集合 Ω 內的整點 $(x_1,\cdots,x_r)$ 對應的函數值．這集合可以是由 r 次元空間中所有的整點所組成，也可以是其中由某些條件所規定的一部份所組成(例如由不等式 $x_1>0,\cdots,x_r>0, x_1\cdots x_r\leqslant N$ 所規定的一部份或座標皆爲素數的點所成的一部分等等)．

若把某種限制加於函數 $f(x_1,\cdots,x_r)$ 或集合 Ω，我們就可從提得這樣籠統的問題得到各種各樣比較特殊的問題，我們現在從這些問題裏選出三個在數論中非常重要的問題．這幾個問題不僅在問題的提法上有相似之處；即在我們用來解決這些問題的方法上也有很多共同的地方．這方法是我在 1934 年發現的；在 1937 年，我曾初次嘗試把它作有系統的敍述．其後，這個方法又經過了重大的修改，個別的結果簡化改進得很厲害．本書裏即將對我的方法及其在所述三個問題上的應用給與一個新的改善了的說明．

我們現在來對所述的三個問題作一個比較詳細的描寫．順便也敍述一下它們發生的簡短歷史，說一下在我 1934 年的方法出現之前用來解決這些問題的方法．

1. 指數函數

$$f(x_1,\cdots,x_r)=e^{2\pi iF(x_1,\cdots,x_r)}$$

的值的分佈問題非常重要，這裏的 $F(x_1,\cdots,x_r)$ 是一個實函數；設集合 Ω 中點的數目 T 爲有限，作函數 $f(x_1,\cdots,x_r)$ 在 Ω 上所有的值之和

$$S=\sum_{\Omega}f(x_1,\cdots,x_r)=\sum_{\Omega}e^{2\pi iF(x_1,\cdots,x_r)},$$

則確定 $|S|$ 的上界也是這些問題裏一個很主要的問題．函數 $f(x_1,\cdots,x_r)$ 的每一個值的絕對值皆等於 1，值的個數等於 T．因此，對於 $|S|$，我們有"平凡估值"

$$|S|\leqslant T,$$

而在這裏，等號成立的充分和必要的條件是函數 $F(x_1,\cdots,x_r)$ 的一切值皆具有同一分數部份．然而，對於異常廣泛的許多種函數 $F(x_1,\cdots,x_r)$ 及集合 Ω 來說，是有可能對於 $|S|$ 建立起比所說的平凡估值來得無比精確的上界，即形如

$$|S| \leqslant T\gamma$$

的上界，此處的 γ 隨集合 Ω 中點數 T 的增大及函數 $F(x_1,\cdots,x_r)$ 的形狀可能同時發生的變化而趨於零．使得這樣的上界與平凡估值區別開來的這一因子 γ，我們將稱之爲“低化因子”（понижающий множитель）.

我們只詳細討論形如

$$\sum e^{2\pi i F(x)}$$

的和數，在這裏，就 x 所求的和係展布於某一區間 $Q \leqslant x < Q+P$ 內的一切整數或這些整數的某一部份．這樣的和數是和數 S 當 $r=1$ 時的特別情形．

形如

$$S=\sum_{x=0}^{q-1} e^{2\pi i \frac{\Phi(x)}{q}}; \qquad \Phi(x)=a_n x^n+\cdots+a_1 x \tag{1}$$

的和數已經研究得非常好，這裏 $q>0$，$(a_n,\cdots,a_1,q)=1$．這種形狀的第一個不平凡的和數，卽形如

$$\sum_{x=0}^{q-1} e^{2\pi i \frac{ax^2}{q}}; \qquad (a,q)=1$$

的和數還是高斯[1] 就已經研究過的，因而有“高斯和數”之名．估計和數（1）的最精確最一般的方法是由莫德爾（Mordell[2]）所得出的，對於素數 q，他得到了估值

$$S \ll q^{1-\nu}.$$

對於一般的情形，華羅庚[3] 曾經得到了估值

$$S \ll q^{1+\varepsilon-\nu}.$$

然而，對於無限多的情形，後面這一估值已經不可能再有重大的改進；可以指出無限多的數值 q，對於其中每一個（本書第二章引理 4），所有形如

$$S=\sum_{x=0}^{q-1} e^{2\pi i \frac{ax^n}{q}}; \qquad (a,q)=1 \tag{2}$$

的和數皆等於 $q^{1-\nu}$.

運用與我們用來估計和數（2）的方法相近的方法，我們也可以估計和數

$$\sum_{x=0}^{q-1} e^{2\pi i \frac{f(x)}{q}}; \quad \sum_{x=0}^{q-1} \chi(f(x)); \qquad f(x)=a_n x^n+\cdots+a_1 x+b_1 x_0+\cdots+b_m x_0^m,$$

這裏的 $a_n,\cdots,a_1$, $b_1,\cdots,b_m$ 是整數，x_0 是由 $xx_0\equiv 1 \pmod q$ 所規定，χ 則是關於模 q 的非主特徵. 利用類似的方法,我們也可以估計許多別的和數. 在本書裏我們不考慮這一類的和數[4-6].

更一般形式的和數

$$S=\sum_{x=Q}^{Q+P-1} e^{2\pi i F(x)};\qquad F(x)=\alpha_n x^n+\cdots+\alpha_1 x \tag{3}$$

的估值是難求得多,這裏的 Q 和 P 是整數，$P>0$，而 $\alpha_n,\cdots,\alpha_1$ 則是實數. 外爾 (H. Weyl) 得到了第一個估計這種和數的普遍方法;因此,這種和數稱爲"外爾和數". 利用外爾氏方法所得到的估值是和利用有理分數對多項式 $F(x)$ 的首項係數所作的近迫有關. 設

$$\alpha_n=\frac{a}{q}+\frac{\theta t}{q^2};\qquad (a,q)=1;\qquad q>0,\ t\geqslant 1.$$

則用外爾氏方法卽得估值[7]

$$|S|\leqslant P\gamma;\qquad \gamma\ll P^{\varepsilon}(P^{-1}+tq^{-1}+tP^{-n+1}+qP^{-n})^{\rho};\qquad \rho=\frac{1}{2^{n-1}}. \tag{4}$$

要想更清楚地表示出這一估值的精確度,我們現在來考慮一種特殊情況: $q\leqslant P$, $t=1$. 根據所說的估值,利用簡單的計算,我們容易得出

$$|S|\ll P^{1+\varepsilon}\gamma';\qquad \gamma'\ll q^{-\rho'};\qquad \rho'=\rho-\varepsilon. \tag{5}$$

數 ε 可以取得很小,使得它在與 ρ 比較起來簡直無足輕重. 現令 P 無限增大,同時也令 q 按某種規律增大. 則低化因子 γ' 將趨於 0，而其接近於 0 的速度則以 ρ' 大到何種程度爲轉移. 但當 n 增大時，關於 n 之階爲 2^{-n} 的 ρ' 很快就接近於 0. 因此,對於大數 n，估值 (5) 非常粗糙.

在本書裏(第六章),運用我的方法,我們對於外爾和數得出了新的估值,根據這一估值,估值 (5) 中的數 ρ' 可以用數

$$\rho_1=\frac{1}{3(n-1)^2\ln 12n\,(n-1)}$$

來代替.

當 n 增大時，關於 n 之階爲 $(n^2\ln n)^{-1}$ 的數 ρ_1，其趨於 0 的速度比 ρ' 來得無比的慢,因此,當 n 很大時,用 ρ_1 代替 ρ'，將給估值 (5) 以更無比的精確估值.

我估計外爾和數的方法的一些有成就的變體，是由萬•德爾•科爾普特 (van der Corput)(這一變體是在 1936 年六月寄來的信裏通知我的)和 B. 林尼克 (1942 年)

得出的．但在這裏，我僅討論與我的著作中所闡述者相近的變體．

和數（2）也屬於所述特殊情形 $q \leqslant P$，$t=1$ 的外爾和數（此時 $Q=0$，$P=q$，$F(x)=\frac{ax^n}{q}$），如我們上面所說，對於其中無限多的和數，等號 $S=q^{1-\nu}=qq^{-\nu}$ 成立．後面這一事實已經指出，在公式（5）中，數 ρ' 已經不可能用任何大於 $\nu=n^{-1}$ 的數去代替，因爲對於無限多的和數（2），這樣的估值已經不正確．

在這裏，這樣的臆測，即估值（5）中的數 ρ' 可以用數 $\nu-\varepsilon$ 來代替，好像是很可能的．這一臆測乃是一個更普遍一些的臆測，即估值（4）中的數 ρ 可以用數 ν 來代替的一種特別情形．利用我的方法底進一步的改進（或用任何別的方法），後面這一臆測的證實或否定看來很有希望．

然而，即使這樣的臆測已經證實，由此到達外爾和數估值問題的完全令人滿意的解決還是非常遙遠．下述非常簡單的研究即可使我們相信這一點．設 s 爲 $1,\cdots,n$ 中的任一數，又設 Q，P 以及多項式 $F(x)$ 的所有係數，除 α_s 之外，皆爲已知．設 α_s 由 0 增到 1．則和數（3）是 α_s 的函數．用記號 $S(\alpha_s)$ 來記此函數．則得

$$\int_0^1 |S(\alpha_s)|^2 d\alpha_s =$$

$$=\sum_{x_1=Q}^{Q+P-1}\sum_{x=Q}^{Q+P-1} e^{2\pi i\left(F(x_1)-F(x)-\alpha_s x_1^s+\alpha_s x^s\right)}\int_0^1 e^{2\pi i\alpha_s\left(x_1^s-x^s\right)} d\alpha_s = P, \tag{6}$$

因爲（第一章引理 4）積分

$$\int_0^1 e^{2\pi i\alpha_s\left(x_1^s-x^s\right)} d\alpha_s$$

當 $x_1=x$ 時等於 1，當 $x_1 \gtrless x$ 等於零．由等式（6），當 $0<\lambda<\frac{1}{2}$ 時，已經不難推出，對於區間 $0\leqslant\alpha_s\leqslant 1$ 中的一切值 α_s，至多除去屬於有限多個總長 $\leqslant P^{2\lambda-1}$（注意 $P^{2\lambda-1}$ 當 P 無限增大時趨於 0）的不相交疊之區間者之外，估值

$$|S(\alpha_s)|^2 \leqslant P^{2-2\lambda}$$

成立，即估值

$$|S(\alpha_s)| \leqslant P^{1-\lambda} \tag{7}$$

成立．表示得概略一點，可以這樣說：對於"幾乎所有的"和數 $S(\alpha_s)$，估值（7）皆成立．

利用第六章的結果，關於和數（3）的絕對值的分佈也可以導出別的重要結論．例如我們可以證明這樣的定理：設 $n>11$，又設 P 與 Q 爲已知．對於 n 次元

立方體 $0 \leqslant \alpha_n \leqslant 1, \cdots, 0 \leqslant \alpha_1 \leqslant 1$ 中之任何一點 $(\alpha_n, \cdots, \alpha_1)$，至多除去屬於有限個總體積 $\leqslant P^{-0.125n^2}$ 的不相交疊之區域者之外，估值

$$|S(\alpha_n, \cdots, \alpha_1)| \ll P^{0.975}$$

皆成立.

設點 $(\alpha_n, \cdots, \alpha_1)$ 所對應的 $|S(\alpha_n, \cdots, \alpha_1)|$ 不是正常那樣大小，要儘量精確的去闡明包含此種 $(\alpha_n, \cdots, \alpha_1)$ 的區域所處的位置，乃是外爾和數估值問題中一個非常重要的任務.

可以用來導出外爾和數估值的方法，也可以用來導出形如

$$S = \sum_{x=Q}^{Q+P-1} e^{2\pi i F(x)} \tag{8}$$

的和數的估值，這裏的 Q 和 P 是整數，$P > 0$，且函數 $F(x)$ 在區間 $Q \leqslant x \leqslant Q+P$ 內 n 次可微分，並滿足條件

$$\frac{1}{A} \leqslant \frac{F^{(n)}(x)}{n!} \leqslant \frac{c}{A},$$

此處的 $A \geqslant 2$. 這種和數在解決素數分佈問題時具有極其重要的應用[9]. 在 $n=2$ 時的特殊情形，這種情形在解決平面上或空間中已與區域內(比如由不等式 $x^2+y^2 \leqslant r^2$ 規定之區域，或由不等式 $x^2+y^2+z^2 \leqslant r^2$ 所規定之區域等等) 的整點數目的問題，具有非常重要的應用. 估計這種和數的方法已經由萬·德爾·科爾普特[10] 和我[11] 各自獨立地得出，同時，萬·德爾·科爾普特還指出，在某種附帶條件之下，與外爾方法結合起來，這種方法還可以弄得精確一些. 運用外爾方法，萬·德爾·科爾普特對於一般情形也得出和數 (8) 的估值[12].

在本書裏(第六章)，當 $n > 11$ 時，在條件 $P \ll A \ll P^{2+2\nu}$ 之下，運用我的方法，我們對於和數 (8) 得出了新的估值

$$S \ll P^{1-\rho}; \qquad \rho = \frac{1}{3n^2 \ln 125n}. \tag{9}$$

當 n 甚大時，這一估值比用外爾方法所得者來得更精密，其更精密的程度，大致與關於估計外爾和數所發生的情形一樣.

人們自然會提出和數 (8) 的估值 (9) 進一步精密化的問題，即在估值 (9) 中，是否可以用可能更大一些的數 $\rho' > \rho$ 去代替 ρ 的問題. 然而，由於我們加於和數 S 的限制太寬大，在這問題上我們很難做出任何確定的臆測. 我想，在這裏最好

是只討論一些重要的特殊例子. 作爲這種例子,我來討論和數(參看第六章定理 2,b 的例)

$$S(t)=\sum_{x=P_0+1}^{P_0+P} e^{i\sigma t\ln x},$$

這裏的 P_0 與P 是滿足條件 $\frac{1}{2}P_0\leqslant P\leqslant P_0$ 的整數, t 是滿足條件 $P_0{}^{n-2}\leqslant t\leqslant P_0{}^{n-1}$ 的數, $\sigma=(-1)^{n+1}$. 於此,我們有

$$F(x)=\frac{\sigma t\ln x}{2\pi};\quad \frac{F^{(n)}(x)}{n!}=\frac{t}{2\pi n x^n};\quad \frac{t}{2\pi n(3P)^n}\leqslant\frac{F^{(n)}(x)}{n!}\leqslant\frac{t}{2\pi n P^n}.$$

因此,設

$$A=\frac{2\pi n(3P)^n}{t};\qquad l=3^n,$$

則有 $P\ll A\ll P^2$, 且在區間 $P_0+1\leqslant x\leqslant P_0+P$ 中,

$$\frac{1}{A}\leqslant\frac{F^{(n)}(x)}{n!}\leqslant\frac{l}{A};$$

因之,我們加於和數 (8) 中的要求在這裏皆已滿足. 再,我們有

$$\int_{P_0^{n-2}}^{P_0^{n-1}}|S(t)|^2dt=\sum_{x_1=P_0+1}^{P_0+P}\sum_{x=P_0+1}^{P_0+P}\int_{P_0^{n-2}}^{P_0^{n-1}}e^{i\sigma t(\ln x_1-\ln x)}dt.$$

但積分

$$\int_{P_0^{n-2}}^{P_0^{n-1}}e^{i\sigma t(\ln x_1-\ln x)}dt$$

當 $x_1=x$ 時等於 $P_0{}^{n-1}-P_0{}^{n-2}$, 當 $x_1\gtrless x$ 時,

$$\ll\frac{1}{|\ln x_1-\ln x|}.$$

在後一種情形,假定 $x_1=x+u$, 則有

$$\ln x_1-\ln x=\ln\left(1+\frac{u}{x}\right)\gg\frac{|u|}{P};\qquad \frac{1}{|\ln x_1-\ln x|}\ll\frac{P}{|u|}.$$

從上所述,當 $n>2$ 時,我們容易得出

$$\int_{P_0^{n-2}}^{P_0^{n-1}}|S(t)|^2dt-P(P_0^{n-1}-P_0^{n-2})\ll P\sum_{u=1}^{P}\frac{P}{u}\ll P^2\ln P,$$

$$\int_{P_0^{n-2}}^{P_0^{n-1}}|S(t)|^2dt=PP_0^{n-1}+O(P_0^{n-1}\ln P).\tag{10}$$

等式 (10) 指出，在估值 (9) 中之數 ρ 已經不可能用數 $\rho' > \frac{1}{2}$ 去代替． 此外這等式也指出，當 $0 < \lambda < \frac{1}{2}$ 時，對於區間 $P_0{}^{n-2} \leqslant t \leqslant P_0{}^{n-1}$ 中之一切值 t，至多除去屬於有限多個總長 $\leqslant P^{n+2\lambda-2}$ (與 $P_0{}^{n-1} - P_0{}^{n-2}$ 比起來毫不足道，其與 $P_0{}^{n-1} - P_0{}^{n-2}$ 之比當 P 無限增大時趨於 0) 之互不相交叠的區間者之外，估值

$$|S(t)|^2 \ll P^{2-2\lambda}$$

成立，卽估值

$$|S(t)| \ll P^{1-\lambda} \tag{11}$$

成立． 表示得粗略一點，可以這樣說：對於“幾乎所有的”和數 $S(t)$，估值 (11) 成立．

最後，我們來討論形如

$$\sum e^{2\pi i F(x)} \tag{12}$$

的和數，這裏的 $F(x)$ 是一實函數，求和記號只展佈於區間 $Q \leqslant x < Q + P$ 上的一部分整數． 我們將要特別加以注意的和數將有 $\gg P^{1-\epsilon}$ 項． 在估計這種和數時，不要以爲所得的估值總是比我們在就展佈於區間 $Q \leqslant x < Q + P$ 上所有的整數求和所得的估值來得壞或來得不好． 例如從和數 (2) 所得到的估值，若令 x 祇跑過區間 $0 \leqslant x < q$ 中與 q 互素的數整，則常常 $\leqslant \sqrt{q}$，其實和數 (2) 對於無限多的數值 q，如我們上面所曾指出，却可以等於 $q^{1-\nu}$.

和數 (12) 的一個特別有趣的特殊情形是形如

$$\sum_{p \leqslant N} e^{2\pi i F(p)} \tag{13}$$

的和數，這裏的 p 跑過素數． 在本書裏(第九章)，就和數 (13) 的最簡單情形，卽當 $F(p) = \alpha p$ 時，我們說明了如何把這種和數的估值問題輕易地化歸成只是我的方法的一種應用．這只須採用下面的恆等式(或此恆等式的某些推廣)就成了：

$$\Phi(1) + \sum_{H < p_1 \leqslant N} \Phi(p_1) = \sum_{dm \leqslant N}\sum \mu(d)\,\Phi(dm), \tag{14}$$

此處 H 是滿足條件 $1 \leqslant H \leqslant \sqrt{N}$ 的任意一數，p_1 跑過不能爲 $\leqslant H$ 的素數所除盡的整數，d 跑過 $\leqslant H$ 的素數之積 (包括“空積”，等於 1) 而 m 則跑過正整數． 恆等式 (14) 是一個很早就知道的恆等式；此恆等式的最初等的證明是根據埃拉多什梯里的篩的觀念． 著名的歐拉恆等式 (p 跑過所有的素數)：

$$\sum_{m=1}^{\infty}\frac{1}{m^s}=\prod_p\frac{1}{1-\frac{1}{p^s}}=\frac{1}{\sum_{d=1}^{\infty}\frac{\mu(d)}{d^s}};\ s=\sigma+it;\ \sigma>1 \tag{15}$$

在某些方面也與恆等式 (14) 相近,恆等式 (15) 及其在函數 $L(s)$ 上的推廣後來就成爲由切褒雪夫、狄里克萊、黎曼、阿達瑪、窪雷·布散，哈代-李托伍德等人[18] 所建立的素數分佈理論的基礎.

恆等式 (15) 正可以由恆等式 (14) 得出,只須令函數 $\Phi(m)$ 等於 m^{-s}、並先令 N，然後再令 H 無限增大即可. 這裏必須注意,將埃拉多什梯里篩法觀念加以某些修改,後來也就造成了著名的"B. 布朗方法",這使得素數分佈理論中很多重要的精緻問題能够得到解決.

2. 實函數 $F(x_1,\cdots,x_r)$ 的分數部分

$$f(x_1,\cdots,x_r)=\{F(x_1,\cdots,x_r)\}$$

的分佈問題與所論的問題 1 密切有關. 也如在問題 1 中一樣,我們在這裏也只限於討論集合 Ω 爲有限的情形. 函數 $f(x_1,\cdots,x_r)$ 的每一個值皆在區間 $0\leqslant f(x_1,\cdots,x_r)<1$ 之內. 原來,對於非常廣泛的許多種函數 $F(x_1,\cdots,x_r)$ 及 集合 Ω, 不管是區間 $0<\alpha<1$ 中的任何數 α, 皆可以用函數 $f(x_1,\cdots,x_r)$ 的值十分精確地去接近於這一 α; 換言之,我們可以證明,從 α 到和它隣近的函數值 $f(x_1,\cdots,x_r)$ 的距離不超過 γ,此處 γ 與 α 無關,且隨集合 Ω 中點的數目 T 的增加及函數 $F(x_1,\cdots,x_r)$ 的形狀可能同時發生的變化而趨於 0. 不但如此，在非常廣泛的情形，我們還可以證明函數 $f(x_1,\cdots,x_r)$ 的值的分佈異常均勻，這就是說，無論區間 $0<\delta<1$ 中的任何一數 δ, $f(x_1,\cdots,x_r)$ 的值,其屬於區間 $0\leqslant f(x_1,\cdots,x_r)<\delta$ 之中者的個數 H 大致是與此區間之長成比例;更精確言之,

$$H=T\delta+O(T\gamma_1),$$

此處的 γ_1 與 δ 無關,且隨集合 Ω 中點的數目 T 的增加及函數 $F(x_1,\cdots,x_r)$ 的形狀可能同時發生的改變而趨於 0. 以後,我們只詳細討論形如 $f(x)=\{F(x)\}$ 的函數的值的分佈,這裏的 x 跑過某一區間 $Q<x\leqslant Q+P$ 中的一切整點或這些整點的某一部分. 這個問題是所說的一般問題當 $r=1$ 時的特殊情形.

函數

$$f(x)=\left\{\frac{\Phi(x)}{q}\right\};\ \Phi(x)=a_nx^n+\cdots+a_1x$$

的值的分佈問題很容易解決，這裏的 $q>1$, $(a_n,\cdots,a_1,q)=1$, 而 x 則跑過關於

模 q 的一完全剩餘系. 在這裏,運用上述和數 (1) 的估值,對於函數 $f(x)$ 之值,其屬於區間 $0 \leqslant f(x) < \delta$ 之中者的個數 H,很容易就可導出漸近公式

$$H = q\delta + O(q^{1+\varepsilon_0-\nu}).$$

函數

$$f(x) = \{F(x)\};\ F(x) = \alpha_n x^n + \cdots + \alpha_1 x \tag{16}$$

的值的分佈問題要難得多,此處的 $\alpha_n, \cdots, \alpha_1$ 是實數,而對於整數 Q 與 P、x 則跑過區間 $Q \leqslant x < Q + P$ 中的一切整數. 這問題的第一個一般的解決是由外爾作出的,他爲了這一目的利用了他所得到的以他的名字來稱呼的和數 (3) 的估值. 但是,外爾自己的估值是很不精確的. 後來,萬·德爾·科爾普特及科克什瑪利用了根據外爾方法所得到的和數 (3) 與 (8) 的最完善的估值,所說的問題主要是在他們的工作裏得到了發展和推廣. 在解決函數 (16) 的值的分佈問題中,運用外爾方法所得到的最精確的結果可以陳述如下: 設

$$\alpha_n = \frac{a}{q} + \frac{\theta}{q^2};\ (a, q) = 1;\ 1 < q < P^n;$$

則數列

$$f(x) = \{F(x)\};\ x = Q, \cdots, Q + P - 1$$

的數中,其屬於區間 $0 \leqslant f(x) < \delta$ 中者的個數 H 可以表成公式[7]

$$H = P\delta + R;\ R \ll P\gamma;\ \gamma = P^{\varepsilon}(P^{-1} + q^{-1} + qP^{-n})^{\sigma};\ \sigma = 2^{-n+1}.$$

在本書裏(第八章),運用我的方法,我們對 R 得出了一個估值,其與所說的估值,相差的程度正如根據我的方法所得到的外爾和數的估值與根據外爾自己的方法所得到的同樣和數的估值相差的程度一樣.

此外(第五章),對於從任意的眞分數 α 到數列

$$f(x) = \{F(x)\};\ x = 1, \cdots, [q_l^{2\lambda}]$$

中與其隣近的數的距離,我們也得出了精確的估值,這裏的 $F(x)$ 具有 (16) 中所說的值,l 是 $n, \cdots, 1$ 中之一數,$\lambda = \frac{1}{l}$,q 則由等式

$$\alpha_l = \frac{a_l}{q_l} + \frac{\theta}{q_l^2};\qquad (a_l, q_l) = 1;\qquad q_l > 0$$

決定.

最後(第十一章),我們用例子 $F(p) = \alpha p$ 來說明我的方法也可能用來解決函數

$$f(p) = \{F(p)\}$$

的值的分佈問題，這裏的 p 跑過區間 $0 < p \leqslant N$ 中的素數.

3. 特別有趣的是函數 $f(x_1, \cdots, x_r)$ 在整點集合 Ω 上所取的值的分佈規律. 在這裏，關於每一個所給的整數 N 就會發生這樣的問題: 在集合 Ω 中有多少個點使得這個 N 成爲函數 $f(x_1, \cdots, x_r)$ 的值;換句話說: 不定方程

$$f(x_1, \cdots, x_r) = N \tag{17}$$

的解答的個數 $I(N)$ 怎樣.

在某些情形，這裏所談的問題只是在確定不等式 $I(N) > 0$，它說明了方程(17)可解;在另外一些情形，則可能對 $I(N)$ 建立起漸近公式;最後，有時也提出求 $I(N)$ 的精確公式的問題等等.

現在我們來更詳細的討論函數

$$f(x_1, \cdots, x_r) = x_1^n + \cdots + x_r^n$$

的值的分佈問題，這裏假定集合 Ω 是由 r 次元空間中具有非負 $x_1, \cdots, x_r$ 的點 $(x_1, \cdots, x_r)$ 所組成.

在這裏，很容易就可證明，當 $r \leqslant n$ 時，存在着無限多個非負的 N 使方程 (17)，卽方程

$$x_1^n + \cdots + x_r^n = N \tag{18}$$

不可解. 實際上，設 N_0 爲一充分大的正整數. 若對任一 $N \leqslant N_0$，等式 (18) 皆成立，則在那裏所出現的每一個 $x_1, \cdots, x_r$ 皆可在下列 $\leqslant N_0^\nu + 1$ 個數目

$$0, 1, \cdots, [N^\nu] \tag{19}$$

中找到. 因此，假若在和數 $x_1^n + \cdots + x_r^n$ 中令所有的 $x_1, \cdots, x_r$ 相互無關的跑過 (19) 中的數，則在此和數的 $[N_0^\nu + 1]^r$ 個值中，我們就得到使得方程 (18) 可解的所有數目 $N \leqslant N_0$. 但使得 (18) 可以以兩兩不同的 $x_1, \cdots, x_r$ 爲解的那種 N，每一個至少遇到 $r!$ 次(數 $x_1, \cdots, x_r$ 可以用 $r!$ 種不同的方法排列). 而使得 (18) 有解，但解 $x_1, \cdots, x_r$ 中必有兩者相等的那種 N 的個數則 $\ll N_0^{\nu(r-1)}$. 因之，使得方程 (18) 有解的全部 $N \leqslant N_0$ 的個數 K 滿足條件

$$K < \frac{(N_0^\nu + 1)^r}{r!} + O(N_0^{\nu(r-1)}) < \frac{(N_0^\nu + 1)^n}{n!} + O(N_0^{1-\nu}) < 0.6 N_0$$

(N_0 充分大). 這就是說，對於多於 $0.4\,N_0$ 個的 $N \leqslant N_0$，方程 (18) 不可解，而這也就證明了我們的說法.

到底什麽樣的 r 使得方程 (18) 對於所有的 $N \geqslant 0$ 有解,或者,至少是對於所有的 $N \geqslant c_0$ 有解,若是 c_0 充分大的時候? 拉格朗日已經指出,方程

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = N$$

在限定 x_1, x_2, x_3, x_4 爲非負整數之下可解. 華林在 1770 年說了這樣的斷言,對於所有 $n > 2$, 存在着這樣的 $r = r(n)$, 它使得方程 (18) 對於一切整數 $N \geqslant 0$ 在限定 $x_1, \cdots, x_r$ 爲非負整數之下可解. 這一斷言享有"華林問題"之名; 它最初是由 D. 希爾柏特在 1909 年所證明. 誠然,希爾柏特用來達到他的目的的方法多少帶有一點專門的性質,並且也很不精確(對於 r 所得到的數目非常大). 因此, 在現刻這個方法差不多已成陳蹟了.

爲了要使得以後的敍述很清楚,我們現在引進記號 $G(n)$ 來討論. 我們用此記號表示具有下述性質的整數: 存在着某一個 c, 使得方程 (18) 當 $r = G(n)$ 時對於所有 $\geqslant c$ 的整數 N 皆可解,但沒有任何 $> c$ 的 c_1 存在,使得方程 (18) 當 $r < G(n)$ 時對所有 $\geqslant c_1$ 的整數 N 皆可解. 由上所述, 立可推知 $G(n)$ 存在, 且在任何場合皆有

$$G(n) > n.$$

在 1919 年,哈代與李托伍德作出了一個解決華林問題的新方法,這與希爾柏特的方法比較起來,簡直是無比的廣泛和精確. 這兩個學者對 $G(n)$ 得出了形如

$$G(n) \leqslant n\, 2^{n-2}\, h \tag{20}$$

的上界,這裏的 h 當 n 無限增大時趨於 1. 此外,對於

$$r \geqslant (n-2)\, 2^{n-1} + 5, \tag{21}$$

哈代與李托伍德首先導出了 $I(N)$ 的漸近公式:

$$I(N) = \frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu)} N^{r\nu-1} \mathfrak{S} + O(N^{r\nu-1-c}), \tag{22}$$

此處的 $\mathfrak{S} = \mathfrak{S}(n, r, N)$ 是"奇異級數",具有在本書中(第二章)所說的值. 哈代與李托伍德也指出了, 在條件 (21) 之下, 有 $\mathfrak{S} \gg 1$. 由學者華羅庚[15] 就哈代與李托伍德方法所得到的最近的精確改進使得不等式 (20) 與 (21) 的右邊可以用數目 $2^n + 1$ 去代替.

在本書裏(第四章), 對於 $G(n)$ 採用我的方法,代替 (20), 我們得出了這樣的上界

$$G(N) < 3n\,(\ln n + 11).$$

這個界在 n 增大時以 $n\ln n$ 的階而增大,因之,關於增大底階來說,已經和我們上面所求出的不可能達到的下界 n 相差很小. 至於漸近公式 (22), 那在本書裏(第七章)我們只證明它當

$$r \geqslant [10n^2 \ln n]$$

時成立. 這樣的一個命題: 將我的方法(但也可能是某種新的方法)加以適當的發展,則 r 的下界的階可能化到 n, 看來是很可能的.

特別有趣的是函數

$$f(p_1, \cdots, p_r) = p_1^n + \cdots + p_r^n$$

的值的分佈問題,這裏的 $p_1, \cdots, p_r$ 跑過素數.

還在 1742 年,在哥特巴赫與歐拉的通信裏就已經提出了所謂"哥特巴赫問題". 它是這樣的一個臆測,就是所有大於 1 的整數皆是不多於三個奇素數之和. 依照這一臆測,則大於 2 的偶數皆必然是兩個奇素數之和. 在 1919 年,布朗在試圖用他自己的方法(關於這個方法,我們在上面已經提到)來解決上述問題時,曾經指出,所有的偶正數皆是兩個數目之和,其各爲不多於 9 個素因子之積. 其後,數目 9 又用數目 4 去代替,但利用這樣的方法來證明哥特巴赫的臆測仍然毫無成就. 在 1930 年, Л. Г. 史尼列爾曼在把他自己關於由正整數所成之集底密率的想法與布朗方法接合在一起之後,即曾指出[16], 所有大於 1 的整數皆是有限定 r 個素數之和;後來又證明了此 r 不超過 67.

在 1923 年,哈代與李托伍德曾經指出解決關於奇數 N 的哥特巴赫問題的方法. 這個方法就其輪廓來說, 與這兩個學者在解決華林問題時所建立者相近. 同時, 哈代與李托伍德在某種條件之下,對於將數目 N 表示成形如

$$N = p_1 + p_2 + p_3$$

的表法的個數 $I(N)$ 導出了漸近公式,這裏的 p_1, p_2, p_3 是素數. 從這漸近公式,哥特巴赫臆測的正確性對於所有充分大的奇數 N 已經立可推出. 哈代與李托伍德的結論其所以帶有條件是在於採用了一些有關 $L(s)$ 函數理論的未經證明的定理. 然而, 使得我們可以對於表出 $I(N)$ 的積分中, 與所謂基本區間對應的那一部分 (參看本書第十章) 導出漸近公式的方法還是到 1937 年初纔做出來的 (佩治[17], 埃什特爾曼[18]). 這個方法不僅用於哥特巴赫問題, 而且也可以用於非常廣泛的類似問題. 由於這個原因, 在 1937 年初就已經解決了一系列的問題: 已經證明了每一充分大的數目 N 皆可表示成 $N = p' + p'' + x^2$ 的形式 (p', p'' 是素數, x 是正

整數)；已經證明了每一充分大的奇數 N 可以表示成 $N = p_1 + p_2 + p_3 p_4$ 的形式(p_1, p_2, p_3, p_4 是素數)等等．然而對於奇數 N 的情形哥特巴赫問題的解決還需要在 $F(p) = \alpha p$ 時和數 (13) 的一個非平凡的估值，也就是需要和數

$$\sum_{p \leqslant N} e^{2\pi i \alpha p}$$

對於區間 $0 \leqslant \alpha \leqslant 1$ 中，其不屬於基本區間內的一切 α 值的一個非平凡的估值．

由我在 1937 年所得到的估計和數 (13) 的普遍方法不僅使我們終於解決了奇數情形的哥特巴赫問題，而且對於許許多多別的同類問題的解決也開闢了道路，比如將整數 N 表示成(素數的華林問題)

$$N = p_1^n + \cdots + p_r^n$$

的形式就是．

在本書裏(第十章)，我們只限於詳細地解決奇數情形的哥特巴赫問題．對於更詳細的介紹問題，我們介紹讀者去看華羅庚的優秀專著[3]．

在結束之際，我將對 K. K. 馬戛里夕威利表示感謝，他曾仔細閱讀此書之原稿，並指出其中存在的許多疏忽之處．

第　一　章

一 般 性 的 引 理

在本章中，我們將提供一些將在以後各章用到的引理．那些顯而易見的，以及衆所週知的引理，我們只加引述，不予證明．引理 10, 15 及 16 是獨創的引理，它的使用乃是本書方法最主要的、帶有原則性的特點．

引理 1, a. 設 r 爲正整數，$x_1, \cdots, x_r$, $y_1, \cdots, y_r$ 爲實數．則

$$(x_1 y_1 + \cdots + x_r y_r)^2 \leqslant (x_1^2 + \cdots + x_r^2)(y_1^2 + \cdots + y_r^2).$$

引理 1, b. 設 r 爲正整數，$m > 1$, $x_1, \cdots, x_r$ 爲非負實數．則

$$(x_1 + \cdots + x_r)^m \leqslant r^{m-1}(x_1^m + \cdots + x_r^m); \quad r^r x_1 \cdots x_r \leqslant (x_1 + \cdots + x_r)^r.$$

證．設 h 爲數目 $x_1, \cdots, x_r$ 的算術平均．在這些數目中，有一個 $\leqslant h$，有一

個 $\geqslant h$. 設 $x_1 \leqslant h \leqslant x_2$. 在區間 $o \leqslant z \leqslant \min(h-x_1, x_2-h)$ 中,函數 $(x_1+z)^m+(x_2-z)^m$ 爲減函數,因而

$$x_1^m + x_2^m \geqslant h^m + (x_1+x_2-h)^m.$$

此外,由 $(x_1-h)(x_2-h) \leqslant 0$, 卽得

$$x_1 x_2 \leqslant h(x_1+x_2-h).$$

按任意次序用字母 $y_2, \cdots, y_r$ 記 $x_1+x_2-h, x_3, \cdots, x_r$, 則我們可以斷言

$$x_1^m + \cdots + x_r^m \geqslant h^m + y_2^m + \cdots + y_r^m; \quad x_1 \cdots x_r \leqslant h y_2 \cdots y_r.$$

在這裏,數目 $y_2, \cdots, y_r$ 的算術平均仍然等於 h. 用同樣方法我們可得

$$y_2^m + \cdots + y_r^m \geqslant h^m + z_3^m + \cdots + z_r^m; \quad y_2 \cdots y_r \leqslant h z_3 \cdots z_r;$$

....

$$u_{r-2}^m + u_{r-1}^m + u_r^m \geqslant h^m + v_{r-1}^m + v_r^m; \quad u_{r-2}u_{r-1}u_r \leqslant h\, v_{r-1} v_r;$$

$$v_{r-1}^m + v_r^m \geqslant h^m + h^m; \qquad v_{r-1} v_r \leqslant h^2.$$

由是卽得

$$x_1^m + \cdots + x_1^m \geqslant r\, h^m; \qquad x_1 \cdots x_r \leqslant h^r,$$

此卽證明引理.

引理 2. 設 η 與 m 爲正整數, $T_1, \cdots, T_\eta$ 爲非負實數. 則

$$\left(\sum_{s=1}^{\eta} 2^{-s} T_s\right)^m \leqslant \sum_{s=1}^{\eta} T_s^m.$$

證. 我們有 (引理 1,b)

$$\left(\sum_{s=1}^{\eta} 2^{-s} T_s\right)^m = 2^{-m}\left(T_1 + \sum_{s=2}^{\eta} 2^{-s+1} T_s\right)^m \leqslant T_1^m + \left(\sum_{s=2}^{\eta} 2^{-s+1} T_s\right)^m.$$

利用同樣方法,我們有

$$\left(\sum_{s=2}^{\eta} 2^{-s+1} T_s\right)^m \leqslant T_2^m + \left(\sum_{s=3}^{\eta} 2^{-s+2} T_s\right)^m;$$

....

$$\left(\sum_{s=\eta-1}^{\eta} 2^{-s+\eta-2} T_s\right)^m \leqslant T_{\eta-1}^m + \left(2^{-\eta+\eta-1} T_\eta\right)^m,$$

由是即證明引理成立.

引理 3. 設 r 爲正整數, $N>0$, $K_r(N)$ 爲不等式

$$x_1^n+\cdots+x_r^n\leqslant N$$

的正整數解 $x_1,\cdots,x_r$ 的組數. 則

$$K_r(N)=T_r N^{r\nu}-\theta r N^{r\nu-\nu};\qquad T_r=\frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu+1)},\qquad \theta>0.$$

證. 顯而易見,

$$K_1(N)=N^\nu-\theta',\quad \theta'>0,$$

故引理對 $K_1(N)$ 成立.

今運用歸納法. 假定對某一 $r\geqslant 1$, 引理對 $K_r(N)$ 成立. 則得 $(\theta''>0,\theta'''>0)$

$$K_{r+1}(N)=\sum_{0<x\leqslant N^\nu}K_r(N-x^n)=T_r\sum_{0<x\leqslant N^\nu}(N-x^n)^{r\nu}-\theta'' r N^{r\nu}=$$

$$=T_r\int_0^{N^\nu}(N-x^n)^{r\nu}dx-\theta'''(r+1)N^{r\nu}=T'N^{(r+1)\nu}-\theta'''(r+1)N^{r\nu};$$

$$T'=T_r\nu\int_0^1(1-z)^{r\nu}z^{\nu-1}dz=T_r\nu\frac{\Gamma(r\nu+1)\Gamma(\nu)}{\Gamma(r\nu+1+\nu)}=T_{r+1}.$$

故引理對 $K_{r+1}(N)$ 亦成立.

引理 4. 設 N 爲整數,

$$I=\int_0^1 e^{2\pi i\alpha N}d\alpha.$$

則

$$I=\begin{cases}1, & \text{若 } N=0,\\ 0, & \text{對於所有其他情形}.\end{cases}$$

引理 5. 設 m 爲大於 1 的整數, a 爲整數,

$$S=\sum_{x=0}^{m-1}e^{2\pi i\frac{ax}{m}}.$$

則

$$S=\begin{cases}m, & \text{若 } a \text{ 能用 } m \text{ 除盡},\\ 0, & \text{在其他情形}.\end{cases}$$

引理 6. 設 M 與 N 爲整數, $M<N$, α 爲非整實數. 則

$$\left|\sum_{x=M}^{N}e^{2\pi i\alpha x}\right|<\frac{1}{2(\alpha)}.$$

證. 我們有

$$\left|\sum_{x=M}^{N} e^{2\pi i\alpha x}\right| = \left|\frac{e^{2\pi i\alpha(N+1)} - e^{2\pi i\alpha M}}{2\,i\,e^{\pi i\alpha}\sin\pi\alpha}\right| \leqslant \frac{1}{|\sin\pi\alpha|} = \frac{1}{\sin\pi(\alpha)} \leqslant \frac{1}{2(\alpha)}.$$

引理 7. 設 $\tau \geqslant 1$. 則任何實數 α 皆可表成

$$\alpha = \frac{a}{q} + z,\ (a,q) = 1;\ 0 < q \leqslant \tau;\ |z| \leqslant \frac{1}{q\tau}$$

的形式.

證. 將 α 展開成連分數,我們可以取那種漸近分數,其分母是 α 的諸漸近分數之分母中不超過 τ 者的最大一個,來作$\frac{a}{q}$.

引理 8, a. 設 f 與 q' 爲整數.

$$\Phi(y) = \frac{ay + \psi(y)}{q},\ (a,q) = 1;\ 0 < q' \leqslant q;\ \lambda \geqslant 0,$$

這裏的 y 跑過值 $y = f, \cdots, f + q' - 1$, 對於這些值,函數 $\psi(y)$ 取實值,其最大者與最小者之差不超過 λ.

α) 設 $U \geqslant 1$,

$$\Omega = \sum_{y} \min\left(U, \frac{1}{2(\Phi(y))}\right); \qquad \Omega_0 = \sum_{y} \min\left(U^2, \frac{1}{4(\Phi(y))^2}\right).$$

則

$$\Omega < (\lambda+3)\,U + q\ln q; \qquad \Omega_0 < (\lambda+3)\,U^2 + 2\,q\,U.$$

β) 設 $V \geqslant 0$, 又設 T 爲滿足條件

$$(\Phi(y)) \leqslant V\,q^{-1}$$

的 y 值的個數. 則

$$T < \lambda + 2 + 2\,V.$$

證. 令 $y = f + z$, 則有

$$(\Phi(y)) = \left(\frac{az + \delta(z)}{q}\right); \qquad \delta(z) = af + \psi(f+z).$$

存在着某一數 B, 使得對於所有的 $z = 0, \cdots, q' - 1$, 有 $B \leqslant \delta(z) \leqslant B + \lambda$. 設 $\beta = \{B\}$, 又用字母 ρ 來記 $az + [B]$ 關於模 q 的最小正剩餘,則得

$$(\Phi(y)) = \left(\frac{\rho + \sigma(\rho)}{q}\right); \qquad \beta \leqslant \sigma(\rho) \leqslant \beta + \lambda.$$

α) 當 $q \leqslant \lambda + 3$ 時, 引理顯然成立; 因此我們只須考慮 $q > \lambda + 3$ 的情形. 對於異於 $\rho = q - [\beta + \lambda + 1], \cdots, q - 1, 0$ 之 $< \lambda + 3$ 個 ρ 值,假定 $\rho = q -$

$[\beta+\lambda+1]-\rho_1$, 並於 $\rho+\sigma(\rho)<\frac{q}{2}$ 時,取 $s=\rho$, 於 $\rho+\sigma(\rho)\geqslant\frac{q}{2}$ 時, 取 $s=\rho_1$, 則有

$$(\Phi(y))\geqslant\frac{s}{q};\qquad \frac{1}{2(\Phi(y))}\leqslant\frac{q}{2s};\qquad \frac{1}{4(\Phi(y))^2}\leqslant\frac{q^2}{4s^2}.$$

因之,在估計 Ω_0 時,假定 $\frac{q}{2U}=\tau$,則得

$$\Omega<(\lambda+3)U+\sum_{s=1}^{[\frac{1}{2}(q-1)]}\frac{q}{s}<(\lambda+3)U+$$

$$+q\sum_{s=1}^{[\frac{1}{2}(q-1)]}\ln\frac{2s+1}{2s-1}<(\lambda+3)U+q\ln q.$$

$$\Omega_0<(\lambda+3)U^2+2\int_0^\tau U^2\,ds+\int_\tau^\infty\frac{q^2}{2s^2}\,ds=(\lambda+3)U^2+2qU.$$

β) 當 $q<\lambda+2+2V$ 時, 引理顯然成立; 當 $q\geqslant\lambda+2+2V$ 時, 引理可由下之事實推出,即不等式 (1) 只當

$$\rho=q-[\beta+\lambda+V],\ \cdots,\ q-1;\ 0,\ \cdots,\ [V]$$

時始有成立之可能.

引理 8, b. 設

$$\alpha=\frac{a}{q}+\frac{\theta}{q^2};\quad (a,q)=1;\quad 2<q\leqslant W;\quad 1<W_0\leqslant W,$$

$$S=\sum_{0<z\leqslant W_0}\min\left(\frac{W}{z},\ \frac{1}{2(\alpha z)}\right).$$

則

$$S\leqslant(W_0+3.5\,q+12\,W\,q^{-1})\ln W.$$

證. 我們可將和數 S 按分法

$$S=\sum_{0<z\leqslant\frac{1}{2}q}+\sum_{\frac{1}{2}q<z\leqslant\frac{3}{2}q}+\cdots+\sum_{(s_0-\frac{1}{2})q<z\leqslant W_0}$$

分成若干項. 對於在第一項中出現的 z, 我們用 ρ 來記 az 關於模 q 的最小非負剩餘. 則易得出

$$(\alpha z)=\left(\frac{\rho+\frac{1}{2}\theta_0(\rho)}{q}\right).$$

由是,若令

$$s=\begin{cases}\rho, \text{若 } \rho\leqslant\frac{1}{2}q, \\ q-\rho, \text{若 } \rho>\frac{1}{2}q,\end{cases}$$

則得

$$(\alpha z)\geqslant\frac{s-\frac{1}{2}}{q}.$$

因之,所說分法中之第一項將

$$\leqslant q\sum_{0<s\leqslant\frac{1}{2}q}\frac{1}{s-\frac{1}{2}}<2q+q\sum_{1<s\leqslant\frac{1}{2}q}\ln\frac{(s-\frac{1}{2})+\frac{1}{2}}{(s-\frac{1}{2})-\frac{1}{2}}<3q\ln q.$$

運用引理 8, a, α 於餘下的其他各項,則得

$$S<3q\ln q+\sum_{s=1}^{s_0}\left(\frac{4W}{(s-\frac{1}{2})q}+q\ln q\right)<$$

$$<(3q+s_0q)\ln q+\frac{4W}{q}\left(2+\sum_{s=2}^{s_0}\ln\frac{(s-\frac{1}{2})+\frac{1}{2}}{(s-\frac{1}{2})-\frac{1}{2}}\right)\leqslant$$

$$\leqslant(W_0+3.5q)\ln W+\frac{12W}{q}\ln W.$$

引理 8, c. 設 P, s, m 爲整數, $P>1$; $s>1$; $m>0$; $k\geqslant 1$,

$$\alpha=\frac{am}{q}+\frac{\theta m}{q^2};\qquad (a,q)=1;\qquad 0<q<P^s,$$

y 跑過 $\leqslant P$ 個相繼的整數, H 爲滿足條件

$$(\alpha y)\leqslant kP^{-s+1} \tag{2}$$

的 y 值的個數. 則

$$H<(3m+2kqP^{-s+1})(Pq^{-1}+1).$$

證. 設 $(m, q)=d$, $m=m_1d$, $q=q_1d$. 則得

$$\alpha=\frac{am_1}{q_1}+\frac{\theta m_1}{q_1q}.$$

在 $\leqslant q_1$ 個相繼的 y 值中,由引理 8, a, β, 其滿足條件 (2) 的 y 的個數將

$$\leqslant m_1+2+2kq_1P^{-s+1}.$$

因之

$$H<(m_1+2+2kq_1P^{-s+1})(Pq_1^{-1}+1)\leqslant(3m+2kqP^{-s+1})(Pq^{-1}+1).$$

引理 9. 設 N與Y爲整數, $Y>1$, $A\geqslant 2\beta\geqslant 2$, y 跑過值 $y=N,\cdots,N+Y-1$,

對於這些值，函數 $\Phi(y)$ 取實值，且當 $y_2-y_1=1$ 時，有

$$\frac{1}{A}\leqslant\Phi(y_2)-\Phi(y)\leqslant\frac{\beta}{A}.$$

α）設 $U\geqslant 1$,

$$S=\sum_{y=N}^{N+Y+1}\min\left(U^2,\frac{1}{4(\Phi(y))^2}\right).$$

則

$$S\leqslant[Y\beta A^{-1}+1](2U^2+2AU).$$

β）設 $W\geqslant 1$, H 爲滿足條件

$$(\Phi(y))\leqslant WA^{-1}$$

的 y 值的個數．則

$$H<[Y\beta A^{-1}+1](2W+1).$$

證．對於給定的實數 α 與整數 h，不可能存在多於一個 y 值，滿足不等式

$$\alpha+h<\Phi(y)\leqslant\alpha+A^{-1}+h. \tag{3}$$

因此，滿足條件

$$\alpha<\Phi(y)\leqslant\alpha+A^{-1}\pmod 1 \tag{4}$$

的 y 值的個數 T 即等於使得不等式(3)可解的 h 值的個數．故得 $T\leqslant h_2-h_1+1$，此處 h_2 與 h_1 分別爲這種 h 的最大值及最小值．但顯而易見，

$$\Phi(N)\leqslant\alpha+A^{-1}+h_1;\qquad \alpha+h_2<\Phi(N+Y-1),$$

由此不難得出

$$h_2-h_1-A^{-1}<\Phi(N+Y-1)-\Phi(N)\leqslant\beta A^{-1}(Y-1);$$
$$T<\beta A^{-1}(Y-1)+A^{-1}+1\leqslant Y\beta A^{-1}+1.$$

α）當 $0<\{\Phi(y)\}\leqslant\frac{1}{2}$ 時，在數列 $s=0,\cdots,[\frac{1}{2}A]$ 中可以找到這樣的 s，使得對於 $\alpha=sA^{-1}$，y 滿足條件(4)，而當 $\{\Phi(y)\}>\frac{1}{2}$ 及 $\{\Phi(y)\}=0$ 時，在同一數列中，可以找到這樣的 s，使得對於 $\alpha+A^{-1}=1-sA^{-1}$，y 滿足條件(4)．同時，在兩種情形之下，皆有 $(\Phi(y))\geqslant sA^{-1}$．因之

$$S<[Y\beta A^{-1}+1]\left(2U^2+\sum_{s=1}^{\infty}\min\left(2U^2,\frac{A^2}{2s^2}\right)\right)<[Y\beta A^{-1}+1](2U^2+2AU).$$

β）所欲證明的結果可以從這樣的事實推出，即長爲 $2WA^{-1}$ 的區間可以用 $[2W+1]$ 個其長 $<A^{-1}$ 的區間來蓋滿．

引理 10, a. 設 $(a,q)=1$, $q>1$,

$$S=\sum_{x=0}^{q-1}\sum_{y=0}^{q-1}{}'\xi(x)\eta(y)e^{2\pi i\frac{a}{q}xy};\qquad \sum_{x=0}^{q-1}|\xi(x)|^2=X_0;\qquad \sum_{y=0}^{q-1}|\eta(y)|^2=Y_0.$$

則

$$|S|\leqslant\sqrt{X_0Y_0q}.$$

證. 我們有(引理 1, a)

$$|S|^2\leqslant X_0\sum_{x=0}^{q-1}\left|\sum_{y=0}^{q-1}\eta(y)e^{2\pi i\frac{a}{q}xy}\right|^2=X_0\sum_{x=0}^{q-1}\sum_{y_1=0}^{q-1}\sum_{y=0}^{q-1}\eta(y_1)\overline{\eta(y)}e^{2\pi i\frac{a}{q}x(y_1-y)}.$$

對於所給定的 y_1 及 y, 就 x 所取的和當 $y_1=y$ 時爲 $q|\eta(y)|^2$, 當 $y_1\neq y$ 時爲零(引理 5). 故 $|S|^2\leqslant X_0Y_0q$, $|S|\leqslant\sqrt{X_0Y_0q}$.

引理 10, b. 設 M, X, N, Y 爲整數, $X>0$, $Y>0$,

$$\Phi(y)=\frac{ay+\psi(y)}{q};\qquad (a,q)=1;\qquad q>0;\qquad \lambda\geqslant 0,$$

y 跑過值 $y=N,\cdots,N+Y-1$; 對於這些值,函數 $\psi(y)$ 取實值,且當 y 跑過任何 $\leqslant q$ 個相繼的數值時,其所對應的值 $\psi(y)$ 之最大者與最小者之差不超過 λ. 又令

$$S=\sum_{x=M}^{M+X-1}\sum_{y=N}^{N+Y-1}\xi(x)\eta(y)e^{2\pi ix\Phi(y)};\qquad \sum_{x=M}^{M+X-1}|\xi(x)|^2=X_0;\qquad \sum_{y=N}^{N+Y-1}|\eta(y)|=Y_1;$$

$$\max|\eta(y)|=\eta.$$

則

$$|S|<\sqrt{X_0Y_1\eta((2\lambda+6)X+3q)[Yq^{-1}+1]}.$$

證. 我們有(引理 1, a)

$$|S|^2\leqslant X_0\sum_{x=M}^{M+X-1}\left|\sum_{y=N}^{N+Y-1}\eta(y)e^{2\pi ix\Phi(y)}\right|^2\leqslant$$

$$\leqslant\frac{X_0}{X}\sum_{x_1=M}^{M+X-1}\sum_{x_2=-X+1}^{X-1}\left|\sum_{y=N}^{N+Y-1}\eta(y)e^{2\pi i(x_1+x_2)\Phi(y)}\right|^2,$$

蓋對於每一給定的 $x=M,\cdots,M+X-1$, 滿足條件 $x_1+x_2=x$ 的 x_1, x_2 恰好有 X 對. 由是(引理 6)

$$|S|^2\leqslant\frac{X_0}{X}\sum_{x_1=M}^{M+X-1}\sum_{x_2=-X+1}^{X-1}\sum_{y_1=N}^{N+Y-1}\sum_{y=N}^{N+Y-1}\eta(y_1)\overline{\eta(y)}e^{2\pi i(x_1+x_2)(\Phi(y_1)-\Phi(y))}\leqslant$$

$$\leqslant\frac{X_0}{X}\sum_{y_1=N}^{N+Y-1}|\eta(y_1)|\sum_{y=N}^{N+Y-1}\eta\min\left(2X^2,\frac{1}{4(\Phi(y_1)-\Phi(y))^2}\right).$$

但 y 的值可以分成 $\leqslant [Y q^{-1}+1]$ 個集合,其各由 $\leqslant q$ 個相繼的 y 值組成. 運用引理 8, a 於每一集合 (取 $\Phi(y)-\Phi(y_1)$ 代 $\Phi(y)$, 取 $X\sqrt{2}$ 代 U),則得

$$|S|^2 < \frac{X_0}{X} Y_1 \eta((\lambda+3)\, 2X^2 + 2qX\sqrt{2})\, [Yq^{-1}+1] <$$

$$< X_0 Y_1 \eta((2\lambda+6) X + 3q)\, [Yq^{-1}+1].$$

引理 10, c. 設 M, X, N, Y 爲整數, $X>0$, $Y>0$, $A \geqslant 2\beta \geqslant 2$, y 跑過值 $y=N, \cdots, N+Y-1$, 對於這些值,函數 $\Phi(y)$ 取實值,且當 $y_2-y_1=1$ 時, 有

$$\frac{1}{A} \leqslant \Phi(y_2)-\Phi(y_1) \leqslant \frac{\beta}{A}.$$

又令

$$S = \sum_{x=M}^{M+X-1} \sum_{y=N}^{N+Y-1} \xi(x)\, \eta(y)\, e^{2\pi i x \Phi(y)}; \qquad \sum_{x=M}^{M+X-1} |\xi(x)|^2 = X_0;$$

$$\sum_{y=N}^{N+Y-1} |\eta(y)| = Y_1; \qquad \max |\eta(y)| = \eta.$$

則

$$|S|^2 \leqslant \sqrt{X_0 Y_1 \eta(4X+3A)\, [Y\beta A^{-1}+1]}.$$

證. 我們有 (參看引理 10, b 的證明)

$$|S|^2 \leqslant \frac{X_0}{X} \sum_{y_1=N}^{N+Y-1} |\eta(y_1)| \sum_{y=N}^{N+Y-1} \eta \min\left(2X^2, \frac{1}{4(\Phi(y_1)-\Phi(y_2))^2}\right),$$

由是,運用引理 9, α, 卽得

$$|S|^2 < \frac{X_0}{X} Y_1 \eta(4X^2+2AX\sqrt{2})\, [Y\beta A^{-1}+1] < X_0 Y_1 \eta(4X+3A)\, [Y\beta A^{-1}+1].$$

引理 11 (富理級數). 設 $F(x)=P(x)+iQ(x)$ 是一週期爲 1 的函數,又設區間 $0<x\leqslant 1$ 可以分成有限多個區間,在每一區間內,函數 $P(x)$ 與 $Q(x)$ 爲連續且單調. 在函數的每一斷點,又令

$$F(x) = \frac{F(x-0)+F(x+0)}{2}.$$

則

$$F(x) = \frac{a_0}{2} + \sum_{m=1}^{\infty} (a_m \cos 2\pi m x + b_m \sin 2\pi m x),$$

$$a_m = 2\int_0^1 F(\xi) \cos 2\pi m\xi\, d\xi; \qquad b_m = 2\int_0^1 F(\xi) \sin 2\pi m\xi\, d\xi.$$

引理 12. 設 r 爲正整數，α 與 β 爲實數，

$$0 < \Delta < \frac{1}{2}; \quad \Delta \leqslant \beta - \alpha \leqslant 1 - \Delta.$$

則存在以 1 爲週期之函數 $\psi(x)$ 滿足條件:

1. $\psi(x) = 1$，在區間 $\alpha + \frac{1}{2}\Delta \leqslant x \leqslant \beta - \frac{1}{2}\Delta$ 中;

2. $0 \leqslant \psi(x) \leqslant 1$，在區間 $\alpha - \frac{1}{2}\Delta \leqslant x \leqslant \alpha + \frac{1}{2}\Delta$ 及 $\beta - \frac{1}{2}\Delta \leqslant x \leqslant \beta + \frac{1}{2}\Delta$ 中;

3. $\psi(x) = 0$，在區間 $\beta + \frac{1}{2}\Delta \leqslant x \leqslant 1 + \alpha - \frac{1}{2}\Delta$ 中;

4. $\psi(x)$ 可展成形如

$$\psi(x) = \beta - \alpha + \sum_{m=1}^{\infty} (a_m \cos 2\pi m x + b_m \sin 2\pi m x)$$

的富理級數，於此，有

$$|a_m| \leqslant \frac{2}{\pi m}; \quad |b_m| \leqslant \frac{2}{\pi m},$$

$$|a_m| \leqslant 2(\beta - \alpha); \quad |b_m| \leqslant 2(\beta - \alpha),$$

$$|a_m| < \frac{2}{\pi m}\left(\frac{r}{\pi m \Delta}\right)^r; \quad |b_m| < \frac{2}{\pi m}\left(\frac{r}{\pi m \Delta}\right)^r.$$

證. 我們現來討論以 1 爲週期之函數 $\psi_0(x)$，其定義如下:

$$\psi_0(x) = 1, \text{ 在區間 } \alpha < x < \beta \text{ 內},$$

$$\psi_0(x) = \frac{1}{2}, \text{ 當 } x = \alpha \text{ 及 } x = \beta,$$

$$\psi_0(x) = 0, \text{ 在區間 } \beta < x < 1 + \alpha \text{ 內}.$$

將此函數展成富理級數，則得

$$\psi_0(x) = \frac{1}{2} a_{0,0} + \sum_{m=1}^{\infty} (a_{m,0} \cos 2\pi m x + b_{m,0} \sin 2\pi m x),$$

$$a_{0,0} = 2\int_{\alpha}^{\alpha+1} \psi_0(x)\, dx = 2\int_{\alpha}^{\beta} dx = 2(\beta - \alpha),$$

$$a_{m,0} = 2\int_{\alpha}^{\beta} \cos 2\pi m x\, dx = \frac{\sin 2\pi m\beta - \sin 2\pi m\alpha}{\pi m},$$

$$b_{m,0} = 2\int_{\alpha}^{\beta} \sin 2\pi m x\, dx = \frac{\cos 2\pi m\alpha - \cos 2\pi m\beta}{\pi m}.$$

令 $\Delta = 2r\delta$，當 $\rho = 1, \cdots, r$ 時，用等式

$$\psi_\rho(x) = \frac{1}{2\delta}\int_{-\delta}^{\delta}\psi_{\rho-1}(x+z)\,dz$$

定義函數 $\psi_\rho(x)$. 運用數學歸納法,不難證明

1. $\psi_\rho(x)=1$, 在區間 $\alpha+\rho\delta\leqslant x\leqslant\beta-\rho\delta$ 內;
2. $0\leqslant\psi_\rho(x)\leqslant 1$, 在區間 $\alpha-\rho\delta\leqslant x\leqslant\alpha+\rho\delta$ 及 $\beta-\rho\delta\leqslant x\leqslant\beta+\rho\delta$ 內.
3. $\psi_\rho(x)=0$, 在區間 $\beta+\rho\delta\leqslant x\leqslant 1+\alpha-\rho\delta$ 內;
4. $\psi_\rho(x)$ 可展成形如

$$\psi_\rho(x)=\beta-\alpha+\sum_{m=1}^{\infty}(a_{m,\rho}\cos 2\pi mx+b_{m,\rho}\sin 2\pi mx)$$

之富理級數,於此有

$$a_{m,\rho}=\frac{\sin 2\pi m\beta-\sin 2\pi m\alpha}{\pi m}\left(\frac{\sin 2\pi m\delta}{2\pi m\delta}\right)^\rho,$$

$$b_{m,\rho}=\frac{\cos 2\pi m\alpha-\cos 2\pi m\beta}{\pi m}\left(\frac{\sin 2\pi m\delta}{2\pi m\delta}\right)^\rho.$$

事實上,假設所有這四個性質對於 $\psi_{\rho-1}(x)$ 皆成立,則其中前三個性質對於 $\psi_\rho(x)$ 顯然成立;第四個性質之成立,可由

$$a_{m,\rho}=2\int_0^1\left(\frac{1}{2\delta}\int_{-\delta}^{\delta}\psi_{\rho-1}(\xi+z)\,dz\right)\cos 2\pi m\xi\,d\xi=$$

$$=\frac{1}{\delta}\int_{-\delta}^{\delta}dz\int_0^1\psi_{\rho-1}(\xi+z)\cos 2\pi m\xi\,d\xi=\frac{1}{\delta}\int_{-\delta}^{\delta}dz\int_0^1\psi_{\rho-1}(\xi)\cos 2\pi m(\xi-z)\,dz=$$

$$=\frac{1}{2\delta}\int_{-\delta}^{\delta}dz\,(a_{m,\rho-1}\cos 2\pi mz+b_{m,\rho-1}\sin 2\pi mz)=a_{m,\rho-1}\frac{\sin 2\pi m\delta}{2\pi m\delta}$$

及

$$b_{m,\rho}=b_{m,\rho-1}\frac{\sin 2\pi m\delta}{2\pi m\delta}$$

得出.

令 $\psi(x)=\psi_r(x)$,我們的引理即已證明.

引理 13 (萬・德爾・科爾普特引理). 設 M 與 M_1 爲整數, $M<M_1$, 又設在區間 $M\leqslant X\leqslant M_1$ 中,實函數 $f(x)$ 的第一、二次導數滿足條件

$$0\leqslant f'(x)\leqslant\frac{1}{2};\qquad f''(x)>0.$$

則當同時取 + 號或同時取 − 號時,我們有

$$\sum_{x=M}^{M_1} e^{\pm 2\pi i f(x)} = \int_M^{M_1} e^{\pm 2\pi i f(x)}\, dx + 2\theta.$$

證. 我們現僅討論 + 號的情形,因爲一號的情形顯然可以化歸這種情形. 運用引理 11 於週期爲 1 的函數 $F(\xi)$, 其在區間 $0 < \xi < 1$ 中係由等式

$$F(\xi) = e^{2\pi i f(x+\xi)}$$

所定義者,則得

$$\frac{e^{2\pi i f(x)} + e^{2\pi i f(x+1)}}{2} - \int_0^1 e^{2\pi i f(x+\xi)}\, d\xi = \frac{e^{2\pi i f(x)} + e^{2\pi i f(x+1)}}{2} - \frac{a_0}{2} =$$

$$= \sum_{m=1}^{\infty} a_m = \sum_{m=1}^{\infty} \int_0^1 e^{2\pi i f(x+\xi)} \left(e^{2\pi i m\xi} + e^{-2\pi i m\xi}\right) d\xi =$$

$$= -\sum_{m=1}^{\infty} \frac{1}{m} \int_0^1 \left(e^{2\pi i m\xi} - e^{-2\pi i m\xi}\right) e^{2\pi i f(x+\xi)} f'(x+\xi)\, d\xi,$$

由是,就所有的 $x = M, \cdots, M_1 - 1$ 求和,卽得

$$\sum_{x=M}^{M_1} e^{2\pi i f(x)} - \frac{1}{2} e^{2\pi i f(M)} - \frac{1}{2} e^{2\pi i f(M_1)} - \int_M^{M_1} e^{2\pi i f(x)}\, dx =$$

$$= -\sum_{m=1}^{\infty} \frac{1}{m} U_m; \qquad U_m = \int_M^{M_1} \left(e^{2\pi i m x} - e^{-2\pi i m x}\right) e^{2\pi i f(x)} f'(x)\, dx.$$

但我們有

$$U_m = \frac{1}{2\pi i} \int_M^{M_1} \frac{f'(x)}{m + f'(x)}\, d e^{2\pi i (mx + f(x))} + \frac{1}{2\pi i} \int_M^{M_1} \frac{f'(x)}{m - f'(x)}\, d e^{2\pi i (-mx + f(x))},$$

由是,依據第二中值定理(將中值定理分別運用於積分的實部分和虛部分),則得

$$|U_m| \leqslant \frac{1}{2\pi} \left(\frac{0.5}{m + 0.5} \sqrt{8} + \frac{0.5}{m - 0.5} \sqrt{8} \right) = \frac{\sqrt{8}}{\pi} \left(\frac{m}{2m-1} - \frac{m}{2m-1} \right).$$

因之,

$$\left| \sum_{x=M}^{M_1} e^{2\pi i f(x)} - \int_M^{M_1} e^{2\pi i f(x)}\, dx \right| \leqslant \frac{1}{2} + \frac{1}{2} + \frac{\sqrt{8}}{\pi} \sum_{m=1}^{\infty} \left(\frac{m}{2m-1} - \frac{1}{2m+1} \right) < 2.$$

引理 14, a. 設 $P \geqslant 1$, z 爲實數,

$$I = \int_0^P e^{2\pi i z x^n}\, dx.$$

則有

$$|I| \leqslant Z; \qquad Z = \begin{cases} P, & 若\ |z| \leqslant P^{-n}, \\ \sqrt{2}\, |z|^{-\nu}, & 若\ |z| > P^{-n}. \end{cases}$$

證． 當 $|z| \leqslant P^{-n}$ 時，引理顯然，故僅討論 $|z| > P^{-n}$ 之情形． 同時，我們將假定 $z > 0$，因爲在被積函數中，用 $-i$ 代 i 並不改變積分之絕對值也．

作變換 $2zx^n = u$，則得

$$I = U + iV; \quad U = \int_0^\sigma \psi(u) \cos \pi u \, du; \quad V = \int_0^\sigma \psi(u) \sin \pi u \, du,$$

$$\sigma = 2zP^n; \quad \psi(u) = \frac{\nu u^{\nu-1}}{(2z)^\nu}; \quad \sigma > 2.$$

令 $k = [\sigma + \frac{1}{2}]$，並將積分區間分成區間 $0 \leqslant u \leqslant \frac{1}{2}$; $\frac{1}{2} \leqslant u \leqslant \frac{3}{2}$; $\frac{3}{2} \leqslant u \leqslant \frac{5}{2}$; $\cdots$, $k - \frac{1}{2} \leqslant u \leqslant \sigma$，我們即將 U 分成積分和

$$U = U_0 + U_1 + U_2 + \cdots + U_k.$$

因 $\psi(u)$ 在區間 $0 < u \leqslant \sigma$ 中爲減函數，故不難明白，$U_1 + U_2 + \cdots + U_k$ 爲一變號級數，其項在數值上漸減，而 $U_0 > 0$，$U_1 < 0$． 因之

$$|U| \leqslant \min(U_0, -U_1) \leqslant \int_0^1 \psi(u) \, du = (2z)^{-\nu}.$$

用同樣方法，可得

$$|V| \leqslant (2z)^{-\nu}.$$

故得

$$|I| \leqslant \sqrt{(2z)^{-2\nu} + (2z)^{-2\nu}} < \sqrt{2}\, z^{-\nu}.$$

引理 14, b. 設 $N \geqslant 2$，$\ln N = r$，z 爲實數，

$$I(z) = \int_2^N \frac{e^{2\pi i z x}}{r} dx; \quad J(x) = \int_2^N \frac{e^{2\pi i z x}}{\ln x} dx.$$

則有

$$I(z) \ll Z; \quad J(z) \ll Z; \quad Z = \begin{cases} Nr^{-1}, & \text{若 } |z| \leqslant N^{-1}, \\ |z|^{-1} r^{-1}, & \text{若 } N^{-1} < |z| \leqslant N^{-\frac{1}{2}}. \end{cases}$$

證． 對於積分 $I(z)$，兩種情形皆顯而易見． 對於積分 $J(z)$，$|z| \leqslant N^{-1}$ 之情形也很顯然；因之，我們僅討論 $N^{-1} < |z| \leqslant N^{-\frac{1}{2}}$ 之情形，且不妨設 $z > 0$．

如證明引理 14, a 時一樣進行討論，我們有（作變換 $2zx = u$）：

$$J(z) = U + iV; \quad U = \int_{\sigma_0}^\sigma \psi(u) \cos \pi u \, du; \quad V = \int_{\sigma_0}^\sigma \psi(u) \sin \pi u \, du;$$

$$\sigma_0 = 4z; \quad \sigma = 2Nz; \quad \psi(u) = \frac{1}{2z \ln \frac{u}{2z}}.$$

$$|U| \leqslant \int_{\sigma_0}^{\sigma_0+1} \psi(u)\,du = \int_2^{2+(2z)^{-1}} \frac{dx}{\ln x} \ll \frac{(2z)^{-1}}{\ln(2+(2z)^{-1})} \ll z^{-1} r^{-1}; \quad V \ll z^{-1} r^{-1}.$$

引理 15. 設 $h, \cdots, l$ 與 k 爲固定整數,

$$0 < h < \cdots < l < n, \quad k > 1,$$

$$M \geqslant 1; \quad p > 1; \quad p_t = p^{(1-\nu)^{t-1}}; \quad t = 1, \cdots, k,$$

對應於每一 t, 作數組系

$$(U_{t,h}, \cdots, U_{t,l}, U_{t,n}),$$

其諸元素 $U_{t,i}$ $(i = h, \cdots, l, n)$ 係由滿足條件

$$U_{t,h} \ll M p_t^h, \cdots, U_{t,l} \ll M p_t^l; \; U_{t,n} \ll M p_t^n$$

之整數所組成,又作數 Φ_t 與 t 對應, Φ_t 的定義是: 無論任何長爲

$$M p_t^{h(1-\nu)}, \cdots, M p_t^{l(1-\nu)}, \; M p_t^{n(1-\nu)}$$

之區間,在所說的數組系中,其元素分別落入這些區間之數組,爲數不超過 Φ_t.

對應於不同的 $t = 1, \cdots, k$, 各取一個組,再就這些組內相應的數之和

$$U_h = U_{1,h} + \cdots + U_{k,h}, \cdots, U_l = U_{1,l} + \cdots + U_{k,l}, \; U_n = U_{1,n} + \cdots + U_{k,n},$$

作成數組

$$(U_h, \cdots, U_l, U_n).$$

則

$$U_h \ll M p_1^h, \cdots, U_l \ll M p_1^l, \; U_n \ll p_1^n, \tag{1}$$

而且,無論對怎樣的整數 $z_h, \cdots, z_l, z_n$, 數組 $(U_h, \cdots, U_l, U_n)$ 中,其滿足條件

$$U_h = z_h, \cdots, U_l = z_l, \; U_n = z_n \tag{2}$$

之組數 $\psi(z_h, \cdots, z_l, z_n)$ 將

$$\ll \Phi_1 \cdots \Phi_k. \tag{3}$$

證. 不等式 (1) 由引理的條件立可得出.

我們現來證明不等式 (3). 在等式 (2) 的條件下,對於給定的 t 及等於 $h, \cdots, l, n$ 中任一數的 r, 我們有

$$U_{t,r} = z_r - U_{1,r} - \cdots - U_{t-1,r} - (U_{t+1,r} + \cdots + U_{k,r}),$$

在這裏,括號中的和數將 $\ll M p^r{}_{t+1} \ll M p_t{}^{r(1-\nu)}$. 這就證明了,當

$$(z_h, \cdots, z_l, z_n),$$
$$(U_{1,h}, \cdots, U_{1,l}, U_{1,n}),$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$(U_{t-1,h}, \cdots, U_{t-1,l}, U_{t-1,n})$$

給定時，系

$$(U_{t,h}, \cdots, U_{t,l}, U_{t,n})$$

中之數必然分别完全落入其長

$$\ll Mp_t^{h(1-\nu)}, \cdots, \ll Mp_t^{l(1-\nu)}, \ll Mp_t^{n(1-\nu)}$$

之某一組區間中，依照引理之條件，這種數組爲數 $\ll \Phi_t$.

逐一對 $t = 1, \cdots, k$ 運用已經證明的事實，則不等式（3）之成立卽已證明.

引理 16. 設 $p = RH$, $R > 1$, $H > 1$, $0 \leqslant X_1$, $X_1 + R \leqslant Y_1$, $Y_1 + R \leqslant X_2$, $\cdots$, $X_n + R \leqslant Y_n$, $Y_n \leqslant p$, $v_1, \cdots, v_n$ 分别跑過區間

$$X_1 < v_1 \leqslant Y_1, \cdots, X_n < v_n \leqslant Y_n$$

中之整數. 則對於無論任何長爲

$$p^{1-\nu}, \cdots, p^{n(1-\nu)}$$

之區間組，數組 $v_1, \cdots, v_n$ 中，其使和數

$$\kappa_1 v_1 + \cdots + \kappa_n v_n, \cdots, \kappa_1 v_1^n + \cdots + \kappa_n v_n^n; \ \kappa_j = \pm 1$$

分别落入該組區間的組數 E 將

$$\ll H^{\frac{n(n-1)}{2}} p^{\frac{n-1}{2}}.$$

證. 設 s 爲滿足條件 $1 < s \leqslant n$ 的整數，又設對於已給定的 $v_{s+1}, \cdots, v_n$, 和數 $\kappa_1 v_1 + \cdots + \kappa_n v_n, \cdots, \kappa_1 v_1^n + \cdots + \kappa_n v_n^n$ 分别落入某一組長爲 $1, p, \cdots, p^{n-1}$ 的區間中. 則和數 $\kappa_1 v_1 + \cdots + \kappa_s v_s, \cdots, \kappa_1 v_1^s + \cdots + \kappa_s v_s^s$ 顯然落入某一組長爲 $1, p, \cdots, p^{s-1}$ 之區間中. 令 $\eta_1, \cdots, \eta_s$; $\eta_1 + \xi_1, \cdots, \eta_s + \xi_s$ 爲兩組具有所設性質的 $v_1, \cdots, v_s$; 則有

$$\kappa_1 \frac{(\eta_1 + \xi_1) - \eta_1}{\xi_1} \xi_1 + \cdots + \kappa_s \frac{(\eta_s + \xi_s) - \eta_s}{\xi_s} \xi_s = \theta_0;$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\kappa_1 \frac{(\eta_1 + \xi_1)^s - \eta_1^s}{s\xi_1} \xi_1 + \cdots + \kappa_s \frac{(\eta_s + \xi_s)^s - \eta_s^s}{s\xi_s} \xi_s = \frac{\theta_{s-1}}{s} p^{s-1},$$

由是卽得

$$\Delta \xi_s \pm \Delta' = 0, \tag{4}$$

$$\Delta = \begin{vmatrix} \frac{(\eta_1+\xi_1)-\eta_1}{\xi_1} & \cdots & \frac{(\eta_s+\xi_s)-\eta_s}{\xi_s} \\ \cdots & \cdots & \cdots \\ \frac{(\eta_1+\xi_1)^s-\eta_1^s}{s\xi_1} & \cdots & \frac{(\eta_s+\xi_s)^s-\eta_s^s}{s\xi_s} \end{vmatrix},$$

$$\Delta' = \begin{vmatrix} \frac{(\eta_1+\xi_1)-\eta_1}{\xi_1} & \cdots & \frac{(\eta_{s-1}+\xi_{s-1})-\eta_{s-1}}{\xi_{s-1}} & \theta_0 \\ \cdots & \cdots & \cdots & \cdots \\ \frac{(\eta_1+\xi_1)^s-\eta_1^s}{s\xi_1} & \cdots & \frac{(\eta_{s-1}+\xi_{s-1})^s-\eta_{s-1}^s}{s\xi_{s-1}} & \frac{\theta_{s-1}}{s}p^{s-1} \end{vmatrix}.$$

在等式 (4) 的右邊逐一對所有的 $\eta_1, \cdots, \eta_s$ 運用拉格朗日公式,則得

$$\Delta_s \xi_s \pm \Delta_s' = 0,$$

$$\Delta_s = \begin{vmatrix} 1 & \cdots & 1 \\ \cdots & \cdots & \cdots \\ x_1^{s-1} & \cdots & x_s^{s-1} \end{vmatrix}, \quad \Delta_s' = \begin{vmatrix} 1 & \cdots & 1 & \theta_0 \\ \cdots & \cdots & \cdots & \cdots \\ x_1^{s-1} & \cdots & x_{s-1}^{s-1} & \frac{\theta_{s-1}}{s}p^{s-1} \end{vmatrix},$$

這裏的 $x_1, \cdots, x_s$ 滿足在引理的陳述中所加於 $v_1, \cdots, v_s$ 的同一不等式.

再,我們有

$$\Delta_s' = \sum_{r=0}^{s-1} \frac{\theta_r p^r}{r+1} U_r,$$

於此, U_r 是在將 Δ_s 展成 x_s 的多項式時, x_s^r 的係數. 但 $\Delta_s = \Delta_{s-1}(x_s - x_1)\cdots(x_s - x_{s-1})$; 故得

$$U_r = D_{s-1-r}\Delta_{s-1},$$

此處的 D_{s-1-r} 是從數 $-x_1, \cdots, -x_{s-1}$ 中,每次取 $s-1-r$ 個作成的積之和,因之, $D_{s-1-r} \ll p^{s-1-r}$. 由是

$$\Delta_s' \ll p^{s-1}\Delta_{s-1}; \quad |\xi_s| \ll \frac{p^{s-1}}{(x_s - x_1)\cdots(x_s - x_{s-1})} \ll H^{s-1}.$$

故知對於給定的 $v_{s+1}, \cdots, v_n$, v_s 取 $\ll H^{s-1}$ 個不同的值. 顯而易見,這樣的結論對於 $s=1$ 也成立. 因之,數組 $v_1, \cdots, v_n$ 中,其使和數 $\kappa_1 v_1 + \cdots + \kappa_n v_n, \cdots, \kappa_1 v_1^n + \cdots + \kappa_n v_n^n$ 屬於任何一組長爲 $1, p, \cdots, p^{n-1}$ 之區間中者,其組數 F

$$\ll 1 \cdot H \cdots H^{n-1} = H^{\frac{n(n-1)}{2}},$$

由是,注意

$$\frac{p^{1-\nu}}{1} \frac{p^{2(1-\nu)}}{p} \cdots \frac{p^{n(1-\nu)}}{p^{n-1}} = p^{\frac{n-1}{2}},$$

則巳容易證明引理成立.

引理 17. 設 k 與 l 爲兩個正整常數, $\tau_k(m)$ 爲方程 $x_1 \cdots x_k = m$ 的正整數解 $x_1, \cdots, x_k$ 的組數 (特別有 $\tau_2(m) = \tau(m)$), E 爲歐拉常數. 則

a. $\tau_k(m) \ll m^{\varepsilon}$;

b. $\sum_{0<m\leqslant z} (\tau_k(m))^l \ll z(\ln z + 1)^{k^l - 1}$;

c. $\sum_{0<m\leqslant z} \tau(m) = z(\ln z + 2E - 1) + O(\sqrt{z})$.

證. 不等式(b)的初等證明巳包含在 K. K. 馬嘎里夕威利的論文中(«Докл. АН СССР», 1939, 二十二卷七期).

第　二　章

奇異級數的研究

在本章裏,我們要來導出"奇異級數" $\mathfrak{S}$ 的若干性質,這些性質,在第四章及第七章中將要用到. 級數 $\mathfrak{S}$ 是由哈代-李托伍德首先予以指出並加以研究.

專用記號. 在本章中,我們將假定 $n \geqslant 3$, 並採用下列記號:

對 $(a, q) = 1$, $q > 1$, 命

$$S_{a,q} = \sum_{x=0}^{q-1} e^{2\pi i \frac{a}{q} x^n}. \tag{1}$$

對正整數 q, 整數 N 及固定正整數 r, 我們用記號 $M(q) = M(q, N, r)$ 來記同餘式

$$x_1^n + \cdots + x_r^n \equiv N \pmod q$$

當 $x_1, \cdots, x_r$ 分別獨立的跑過模 q 的一完全剩餘系時的解答的組數. 此外,令 a 跑過模 q 的一既約剩餘系,我們假定

$$A(q)=A(q,N,r)=q^{-r}\sum_{a}S_{a,q}^{r}e^{-2\pi i\frac{a}{q}N}. \tag{2}$$

我們又令(若下之無限級數收斂)

$$\mathfrak{S}=\mathfrak{S}(N,r)=\sum_{q=1}^{\infty}A(q,N,r). \tag{3}$$

我們用字母 p 表示素數. 衆所週知,當 $p>2$ 時,存在數 g,使得對於所有的整數 $s>0$,g 對模 p^s 屬於指數 $\varphi(p^s)$,而且,對於模 p^s 的既約剩餘系中的任一數,必有一唯一的非負整數 $b<\varphi(p^s)$,使其 $\equiv g^b \pmod{p^s}$. 當 $p=2$ 時,存在數 g,使得對於所有的整數 $s>1$,g 對模 2^s 屬於 $2^{-1}\varphi(2^s)$,而且,對於模 2^s 的既約剩餘系中任一形如 $4m+1$ 的數,必有一唯一的非負整數 $b<2^{-1}\varphi(2^s)$,使其 $\equiv g^b \pmod{2^s}$.

我們用 τ 來記數 n 的規範分解式中 p 的指數. 並假定

$$\gamma=\tau+1,\quad 當\quad p>2,$$
$$\gamma=\tau+2,\quad 當\quad p=2.$$

又令(假若下之無限級數收斂)

$$\psi(p)=\psi(p,N,r)=\sum_{s=0}^{\infty}A(p^s,N,r). \tag{4}$$

引理 1. 設 $q_1,\cdots,q_k$ 兩兩互素,定義 Q_s 如

$$Q_s=q_1\cdots q_k q_s^{-1}.$$

則有

$$S_{a_1,q_1}\cdots S_{a_k,q_k}=S_{a_1Q_1+\cdots+a_kQ_k,q_1\cdots q_k}.$$

證. 我們有

$$S_{a_1,q_1}\cdots S_{a_k,q_k}=\sum_{x_1=0}^{q_1-1}\cdots\sum_{x_k=0}^{q_k-1}e^{2\pi i\left(\frac{a_1}{q_1}+\cdots+\frac{a_k}{q_k}\right)(Q_1x_1+\cdots+Q_kx_k)^n}=$$

$$=\sum_{x_1=0}^{q_1-1}\cdots\sum_{x_k=0}^{q_k-1}e^{2\pi i\frac{a_1Q_1+\cdots+a_kQ_k}{q_1\cdots q_k}(Q_1x_1+\cdots+Q_kx_k)^n},$$

因 $Q_1x_1+\cdots+Q_kx_k$ 跑過模 $q_1\cdots q_k$ 的一完全剩餘系,故引理即已證明.

引理 2. 設 $q_1,\cdots,q_k$ 兩兩互素,則有

$$A(q_1)\cdots A(q_k)=A(q_1\cdots q_k).$$

證. 令 $a_1,\cdots,a_k$ 分別跑過模 $q_1,\cdots,q_k$ 的既約剩餘系,則得(引理 1)

$$A(q_1)\cdots A(q_k)=(q_1\cdots q_k)^{-r}\sum_{a_1}\cdots\sum_{a_k}(S_{a_1,q_1}\cdots S_{a_k,q_k})^r e^{-2\pi i\left(\frac{a_1}{q_1}+\cdots+\frac{a_k}{q_k}\right)N}=$$

$$=(q_1\cdots q_k)^{-r}\sum_{a_1}\cdots\sum_{a_k}S^r_{a_1Q_1+\cdots+a_kQ_k,q_1\cdots q_k}e^{-2\pi i\frac{a_1Q_1+\cdots+a_kQ_k}{q_1\cdots q_k}N},$$

因 $a_1Q_1+\cdots+a_kQ_k$ 跑過模 $q_1\cdots q_k$ 的既約剩餘系，故引理卽已證明.

引理 3. 我們有

$$|S_{a,p}|\leqslant(\delta-1)\sqrt{p}\ ;\quad \delta=(n,p-1).$$

證. 如所週知，當 $(z,p)=1$ 時，同餘式 $x^n\equiv z\ (\mathrm{mod}\ p)$ 可解之充分且必要之條件爲 $\mathrm{ind}\,z$ 可被 δ 除盡，而在可解時，則此同餘式有 δ 個解. 因之，若 $\delta=1$，則有(第一章引理 5) $S_{a,p}=0$; 而若 $\delta>1$，則得

$$|S_{a,p}|=\left|1+\sum_{m=0}^{\delta-1}\sum_{z=1}^{p-1}e^{2\pi i\frac{m\,\mathrm{ind}\,z}{\delta}}e^{2\pi i\frac{az}{p}}\right|=\left|\sum_{m=1}^{\delta-1}\sum_{z=1}^{p-1}e^{2\pi i\frac{m\,\mathrm{ind}\,z}{\delta}}e^{2\pi i\frac{az}{p}}\right|\leqslant$$

$$\leqslant\sqrt{(\delta-1)\sum_{m=1}^{\delta-1}\sum_{z_1=1}^{p-1}\sum_{z=1}^{p-1}e^{2\pi i\frac{m(\mathrm{ind}\,z_1-\mathrm{ind}\,z)}{\delta}}e^{2\pi i\frac{a(z_1-z)}{p}}},$$

由是，對於每一 $t=1,\cdots,p-1$，將根號下之和數中其滿足條件

$$z_1\equiv tz\ (\mathrm{mod}\ p)$$

之項合併，則得

$$|S_{a,p}|\leqslant\sqrt{(\delta-1)\sum_{m=1}^{\delta-1}\sum_{t=1}^{p-1}\sum_{z=1}^{p-1}e^{2\pi i\frac{m\,\mathrm{ind}\,t}{\delta}}e^{2\pi i\frac{a(t-1)z}{p}}}=$$

$$=\sqrt{(\delta-1)\sum_{m=1}^{\delta-1}\left(p-1-\sum_{t=2}^{p-1}e^{2\pi i\frac{m\,\mathrm{ind}\,t}{\delta}}\right)}=$$

$$=\sqrt{(\delta-1)\sum_{m=1}^{\delta-1}p}=(\delta-1)\sqrt{p}.$$

引理 4. 設 α 爲整數，$1<\alpha\leqslant n$, $(n,p)=1$. 則

$$S_{a,p^\alpha}=p^{\alpha-1}.$$

證. 用變換

$$x=p^{\alpha-1}\xi+z$$

變換和數 S_{a,p^α}，此處 ξ 與 z 相互無關地跑過值

$$\xi=0,\cdots,p-1;\qquad z=0,\cdots,p^{\alpha-1}-1,$$

則此和數之項卽化為

$$e^{2\pi i\left(\frac{az^n}{p^a}+\frac{anz^{n-1}}{p}\xi\right)}$$

之形式. 其對應於任一不能為 p 除盡之 z 的各項所成之和等於零. 故和數 S_{a,p^a} 只等於那種項之和, 其 z 為 p 之倍數, 卽 x 為 p 之倍數者. 但此種項為數等於 p^{a-1}, 且其中每一項皆等於 1.

引理 5. 設 a 為整數, $a>n$, $(n, p)=1$. 則

$$S_{a,p^a}=p^{n-1}S_{a,p^{a-n}}.$$

證. 用變換(顯然有 $n\geqslant\tau+2$)

$$x=p^{a-\tau-1}\xi+z$$

變換和數 S_{a,p^a}, 此處 ξ 與 z 相互無關地跑過值

$$\xi=0, \cdots, p^{\tau+1}-1, \quad z=0, \cdots, p^{a-\tau-1}-1,$$

則此和數之項卽化為

$$e^{2\pi i\left(\frac{az^n}{p^a}+\frac{anz^{n-1}}{p^{\tau+1}}\xi\right)}$$

之形式. 其對應於任一不能為 p 除盡之 z 的各項所成之和等於零. 故和數 S_{a,p^a} 只等於那種項之和,其 z 為 p 之倍數,卽 x 為 p 之倍數者. 由是

$$S_{a,p^a}=\sum_{x_1=0}^{p^{a-1}-1}e^{2\pi i\frac{ap^nx_1^n}{p^a}}=\frac{p^{a-1}}{p^{a-n}}\sum_{x_1=0}^{p^{a-n}-1}e^{2\pi i\frac{ax_1^n}{p^{a-n}}}=p^{n-1}S_{a,p^{a-n}}.$$

引理 6. 我們有

$$|S_{a,q}|<n^{n^6}q^{1-\nu}; \quad A(q)\ll q^{1-r\nu}.$$

證. 我們只須證明前一不等式卽可,因後一不等式由此容易推出. 令

$$q=p_1^{a_1}\cdots p_k^{a_k}$$

為數 q 之規範分解式. 我們現引用引理 1, 此時我們令 $q_s=p_s^{a_s}$, 並用同餘式 $a\equiv a_1Q_1+\cdots+a_kQ_k \pmod q$ 來定義 $a_1, \cdots, a_k$ (如所週知,這常常是可能的). 如是,若用等式 $S_{a,q}=q^{1-\nu}T_{a,q}$ 引入記號 $T_{a,q}$, 則得

$$T_{a,q}=T_{a_1,p_1^{a_1}}\cdots T_{a_k,p_k^{a_k}}.$$

但當 $1\leqslant a\leqslant n$, $(p, n)=p$,我們有

$$|T_{a,p^a}|=p^{-a(1-\nu)}|S_{a,p^a}|\leqslant p^{a\nu}\leqslant p\leqslant n;$$

當 $\alpha = 1$, $(p, n) = 1$, 有(引理 3)

$$|T_{a,p^\alpha}| < p^{-(1-\nu)} n \sqrt{p} \leqslant n p^{-\frac{1}{3}};$$

當 $1 < \alpha \leqslant n$, $(p, n) = 1$, 有(引理 4)

$$|T_{a,p^\alpha}| = p^{-\alpha(1-\nu)} p^{\alpha-1} = p^{\alpha\nu-1} \leqslant 1.$$

故當 $1 \leqslant \alpha \leqslant n$ 時,我們常有

$$|T_{a,p^\alpha}| \leqslant \begin{cases} n, \text{ 若 } p \leqslant n^6, \\ 1, \text{ 若 } p > n^6. \end{cases}$$

後一不等式當 $\alpha > n$ 時也成立,蓋由引理 5, 當 $\alpha > n$, 有

$$T_{a,p^\alpha} = p^{-\alpha(1-\nu)} p^{n-1} S_{a,p^{\alpha-n}} = T_{a,p^{\alpha-n}},$$

因而 $\alpha > n$ 之所有 T_{a,p^α} 皆等於某一 $\alpha_0 \leqslant n$ 之 $T_{a,p^{\alpha_0}}$. 由上所證,卽得

$$|T_{a,q}| \leqslant n^{n^6}; \quad |S_{a,q}| \leqslant n^{n^6} q^{1-\nu}.$$

引理 7. 對於整數 $r \geqslant 4n$ 及整數 N, 同餘式

$$x_1^n + \cdots + x_r^n \equiv N \pmod{p^\gamma}$$

在非所有的 $x_1, \cdots, x_r$ 皆能爲 p 除盡之條件下可解.

證. 由於 $N = N - 1 + 1^n$, $0^n = 0$, 故只須在假定 $(N, p) = 1$, $0 < N < p^\gamma$ 之下,證明同餘式

$$x_1^n + \cdots + x_t^n \equiv N \pmod{p^\gamma} \tag{5}$$

對某一 $t \leqslant 4n - 1$ 可解卽可.

若 $p = 2$, 則 $p^\gamma = 2^{\tau+2} \leqslant 4n$. 同餘式 (5) 當 $t = N$ 時可解,因爲我們可以取(比如說)

$$x_1 = \cdots = x_t = 1.$$

設 $p > 2$; 我們現來討論使同餘式 (5) 可解的最小數目 $t = t(N)$. 我們現將數 N 與數列 $v = 0, \cdots, n-1$ 中之一數 v 對應,此 v 是由同餘式 $(s = \gamma)$

$$N \equiv g^b \pmod{p^\gamma}$$

所定義之 b 關於模 n 的最小非負剩餘. 若 N_0 與 N 對應同一個 v, 則有

$$N_0 \equiv g^{b_1} \pmod{p^\gamma}; \quad b_1 \equiv b \pmod{n}; \quad b_1 = b + kn,$$
$$N_0 \equiv N g^{-b+n\varphi(p^\gamma)} . g^{b_1} \equiv N z^n \pmod{p^\gamma}; \quad z = g^{k+\varphi(p^\gamma)},$$

而由 (5), 則得

$$(x_1 z)^n + \cdots + (x_t z)^n \equiv N_0 \pmod{p^\gamma}.$$

此即證明 $t(N_0) \leqslant t(N)$. 同法可證 $t(N) \leqslant t(N_0)$. 故得 $t(N_0) = t(N)$. 因之,與同一 v 對應之諸數 N 皆對應同一的值 $t(N)$. 由是可知,我們可將討論中的所有數目 N 分成 $m(\leqslant n)$ 個集合,具有同一值 $t(N)$ 的數屬於同一集合.

設各個集合的最小代表數,按增加的次序排列時,是

$$N_1, \cdots, N_m.$$

顯而易見,$N_1=1$,因爲1是它所屬集合的最小代表數,而且也是最小的正整數.同時,由於 $1=1^n$,故有 $t(N_1)=1=2-1$. 我們現用歸納法來證明常有 $t(N_j) \leqslant 2j-1$. 設此不等式對 $N_1, \cdots, N_h$ 皆成立. 數 N_{h+1} 是它所屬集合的最小代表數,而數 $N_{h+1}-1$, $N_{h+1}-2$ 中必有一不能爲 p 除盡,故必屬於以 $N_1, \cdots, N_h$ 爲代表數的諸集合之一;因之,$t(N_{h+1}) \leqslant 2h-1+2 \leqslant 2(h+1)-1$. 特別,我們有 $t(N_m) \leqslant$ $\leqslant 2m-1 \leqslant 2n-1 < 4n-1$; 此即證明 $p>2$ 時之引理.

引理 8. 若同餘式

$$y^n \equiv a \pmod{p^\gamma}$$

在 y 不爲 p 除盡之條件下可解,則對整數 $s > \gamma$, 同餘式

$$x^n \equiv a \pmod{p^s}$$

也可解.

證. 我們常可求得非負整數 b, 使

$$a \equiv y^n g^b \pmod{p^s}. \tag{6}$$

特別,由此可以得出 $g^b \equiv 1 \pmod{p^\gamma}$; 因之,對於某一非負整數 b_1, 我們有 $b=p^\tau(p-1)b_1$ 任取一非負整數 k, 我們可以將同餘式(6)中的指數 b 代以新的指數

$$b + kp^{s-1}(p-1) = p^\tau(p-1)(b_1 + kp^{s-1-\tau}).$$

同時,若令 $n = p^\tau n_1$, 則由 $(n_1, p) = 1$, 我們可以取 k 使得括號中的式子是 n_1 的倍數. 於是,所說的新指數即取 $p^\tau n_1 h = nh$ 之形式,此處的 h 是一整數;同餘式(6)則變成

$$y^n g^{nh} \equiv a \pmod{p^s};$$

這也就證明了我們的引理.

引理 9. 設 s 爲整數, $s > \gamma$, $r \geqslant 4n$. 則

$$M(p^s, N, r) \geqslant p^{(s-\gamma)(r-1)}.$$

證. 由引理 7，存在一不爲 p 所除盡之整數 y，及整數 $y_2, \cdots, y_r$，使得

$$y^n \equiv N - y_2^n - \cdots - y_r^n \pmod{p^\gamma}.$$

令數列 $x_2, \cdots, x_r$ 中的每一 x_j 相互獨立的跑過模 p^s 的最小剩餘系中對模 p^γ 與 y_j 同餘的那種數，則得 $p^{(s-\gamma)(r-1)}$ 個數組 $x_2, \cdots, x_r$. 對於每一個這樣的數組，同餘式

$$y^n \equiv N - x_2^n - \cdots - x_r^n \pmod{p^\gamma}$$

皆成立. 故(引理 8) 同餘式

$$x^n \equiv N - x_2^n - \cdots - x_r^n \pmod{p^s}$$

可解. 此卽證明我們的引理.

引理 10. 設 m 爲整數，$m > 0$. 則

$$\sum_{q/m} A(q, N, r) = m^{-(r-1)} M(m, N, r).$$

證. 我們現來討論和數

$$\sum_{a=0}^{m-1} \sum_{x_2=0}^{m-1} \cdots \sum_{x_r=0}^{m-1} e^{2\pi i \frac{a(x_1^n + \cdots + x_r^n - N)}{m}}.$$

此和數等於 $mM(m)$. 將此和數中其 $m(a, m)^{-1}$ 等於同一値 q 的各項合在一起，而當 q 給定時，又令 a_q 跑過模 q 的一旣約剩餘系，則我們對此和數卽得

$$\sum_{q/m} \sum_{a_q} \sum_{x_1=0}^{m-1} \cdots \sum_{x_r=0}^{m-1} e^{2\pi i \frac{a_q(x_1^n + \cdots + x_r^n - N)}{q}} = m^r \sum_{q/m} A(q, N, r).$$

引理 11. 當 $r \geqslant 2n+1$ 時，級數 $\mathfrak{S}(N, r)$ 與 $\psi(p, N, r)$ 絕對收斂，且

$$\mathfrak{S}(N, r) = \prod_p \psi(p, N, r),$$

此處 p 跑過所有的素數.

證. 級數 $\mathfrak{S}(N, r)$ 與 $\psi(p, N, r)$ 之爲絕對收斂，可由引理 6 推出. 再，當 $\xi > 2$ 時，我們有(引理 2)

$$\prod_{p \leqslant \xi} \psi(p, N, r) = \prod_{p \leqslant \xi} \sum_{s=0}^{\infty} A(p^s, N, r) = \sum_{q \leqslant \xi} A(q, N, r) + \sum_{q > \xi}' A(q, N, r),$$

在這裏，第二被加項只包含那種 $A(q, N, r)$，其所對應的 q 値，不能爲任何 $p > \xi$ 所除盡者. 由於 $\mathfrak{S}(N, r)$ 絕對收斂，故當 $\xi \to \infty$ 時，第二被加項趨於零；而第一被

加項則趨於 $\mathfrak{S}(N,r)$.

引理 12. 當 $r\geqslant 4n$ 時,我們有

$$\mathfrak{S}(N,r)\gg 1.$$

證. 由引理 9 及 10, 當 $s>\gamma$ 時,我們有

$$\sum_{q/p^s}A(q,N,r)\geqslant p^{-s(r-1)+(s-\gamma)(r-1)}=p^{-\gamma(r-1)};$$

對 $s\to\infty$ 取極限,則得

$$\psi(p,N,r)\geqslant p^{-\gamma(r-1)}.$$

此外,我們有(引理 6)

$$\psi(p,N,r)-1=\sum_{s=1}^{\infty}A(p^s,N,r)\ll\sum_{s=1}^{\infty}p^{s(1-rv)}\ll p^{-3},$$

故當 $c_0>1$ 充分大時,對於所有的 $p>c_0$,我們有

$$\psi(p,N,r)\geqslant 1-p^{-2}.$$

因之,運用引理 11,即得

$$\mathfrak{S}(N,r)=\prod_{p<c_0}\psi(p,N,r)\prod_{p\geqslant c_0}\psi(p,N,r)\geqslant\prod_{p<c_0}p^{-\gamma(r-1)}\prod_{p\geqslant c_0}(1-p^{-2})\gg 1.$$

第 三 章

一個定積分的研究

在本章中,我們將要對一個定積分之某一部分導出一個在第四章及第七章須要用到的漸近公式,所說的定積分是用來表出以一定多個正整數的 n 次方之和來表示一個整數的表法的種數.

原則上,這個定積分是與哈代-李托伍德在他們的研究中用來表出同一表法的種數所用的積分相近. 我們這裏所作的論證,就其基本觀念來說,是和他們所作的與此相應的論證一致.

專用記號. 在本章中,我們假定 $n\geqslant 3$, 並採用下列記號:

r 是滿足條件 $r\geqslant 2n+1$ 的固定整數.

N 是滿足條件 $N\geqslant C$ 的整數,此處 C 是一充分大的數.

$P=[N^{\nu}]$，$\tau=2nP^{n-1}$，N_0 與 N_1 是整數，滿足條件 $\frac{1}{2}N\leqslant N_0\leqslant N$，$N_0-P^{n-\nu}\leqslant N_1\leqslant N_0$.

β 是滿足條件 $\frac{1}{4}\leqslant\beta\leqslant 1-\nu$ 的一常數.

符號 $W(N_1)$ 是用來記將一數 N_1 表成

$$N_1=x_1^n+\cdots+x_r^n$$

的表法的種數,式中 $x_1,\cdots,x_r$ 是正整數. 依據第一章引理 4，我們有

$$W(N_1)=\int_{-\tau^{-1}}^{-\tau^{-1}+1}L_\alpha^r\,e^{-2\pi i\alpha N_1}d\alpha;\qquad L_\alpha=\sum_{x=1}^{P}e^{2\pi i\alpha x^n}.$$

包含所有滿足條件

$$\alpha=\frac{a}{q}+z;\quad (a,q)=1;\quad -\frac{1}{q\tau}\leqslant z\leqslant\frac{1}{q\tau};\quad 0<q\leqslant P^{\beta};\quad 0\leqslant a<q$$

之 α 的區間稱爲基本區間；從區間 $-\tau^{-1}\leqslant\alpha\leqslant-\tau^{-1}+1$ 中除去基本區間之後所留下的區間叫做餘區間. 不難看出,對應於不同值對 a 與 q 之基本區間不會包含有共同之 α 值. 事實上,由

$$\frac{a}{q}+z=\frac{a_1}{q_1}+z_1;\quad \frac{a}{q}\neq\frac{a_1}{q_1};\quad |z|\leqslant\frac{1}{q\tau};\quad |z|\leqslant\frac{1}{q_1\tau},$$

即得

$$\left|\frac{aq_1-a_1q}{qq_1}\right|\leqslant\frac{2}{\tau};\quad \frac{1}{qq_1}\leqslant\frac{2}{\tau};\quad \frac{1}{P^2}<\frac{1}{3P^2}.$$

積分 $W(N_1)$ 中對應於基本區間之部分,我們用記號 $W_0(N_1)$ 來表示.

除上述記號之外,在本章的論證中,我們還將採用第二章的一些專用記號.

$W_0(N_0)$ 的漸近公式. 設 α 屬於含有分數 $\frac{a}{q}$ 的基本區間. 用變換 $x=qt+s$ 變換和數 L_α，這裏的 s 跑過數目 $s=0,\cdots,q-1$，對於給定的 s，t 則跑過區間

$$-sq^{-1}<t\leqslant(P-s)q^{-1}\tag{1}$$

中的整數. 於是,以 z 表 α，則得

$$L_\alpha=\sum_{s=0}^{q-1}\sum_{t}e^{2\pi i\left(\frac{as^n}{q}+z(qt+s)^n\right)}=$$

$$=\sum_{s=0}^{q-1}e^{2\pi i\frac{as^n}{q}}D_s(z);\quad D_s(z)=\sum_{t}e^{2\pi iz(qt+s)^n}.$$

但在區間 (1) 中,我們有

$$\frac{d}{dt}|z|(qt+s)^n \leqslant \frac{1}{2}.$$

故由第一章引理 13,

$$D_s=\int_{-sq^{-1}}^{(P-s)q^{-1}} e^{2\pi i z(qt+s)^n}\,dt+4\theta'=\frac{1}{q}\int_0^P e^{2\pi i z x^n}\,dx+4\theta',$$

由是,

$$L_a=\psi\frac{S_{a,q}}{q}+4\theta'' q;\qquad \psi=\int_0^P e^{2\pi i z x^n}\,dx. \tag{2}$$

但由第一章引理 14, a 及第二章引理 6, 我們有

$$\psi\frac{S_{a,q}}{q}\ll Z\,q^{-\nu};\qquad Z=\begin{cases}P, \text{若 } |z|\leqslant P^{-n},\\ |z|^{-\nu}, \text{若 } P^{-n}\leqslant |z|.\end{cases}$$

顯而易見, $Zq^{-\nu}>q$, 因之,由 (2),我們即得

$$L_a^r-\left(\psi\frac{S_{a,q}}{q}\right)^r\ll (Z\,q^{-\nu})^{r-1}q\ll q^{-1}Z^{r-1}.$$

但當 $w>0$ 時,我們有 $e^{2\pi i w}-1\ll w$; 故得

$$L_a^r\,e^{-2\pi i a N_1}=$$

$$=\psi^r\left(\frac{S_{a,q}}{q}\right)^r e^{-2\pi i\frac{a}{q}N_1-2\pi i z N_0}+O(q^{-1}Z^{r-1}+q^{-2-\nu}Z^r|z|P^{n-\nu}).$$

由是,對於積分 $W(N_1)$ 中,與包含分數 $\frac{a}{q}$ 的基本區間相應之部分 $H_{a,q}$, 我們有

$$H_{a,q}=R_q(N_0)\left(\frac{S_{a,q}}{q}\right)^r e^{-2\pi i\frac{a}{q}N_1}+F,$$

$$R_q(N_0)=\int_{-(q\tau)^{-1}}^{(q\tau)^{-1}}\psi^r e^{-2\pi i z N_0}\,dz;\quad F\ll\int_0^{(q\tau)^{-1}}(q^{-1}Z^{r-1}+q^{-2-\nu}Z^r z P^{n-\nu})\,dz.$$

再,我們易得

$$\left(\frac{S_{a,q}}{q}\right)^r\left(\int_{-\infty}^{-(q\tau)^{-1}}\psi^r e^{-2\pi i z N_0}\,dz+\int_{(q\tau)^{-1}}^{\infty}\psi^r e^{-2\pi i z N_0}\,dz\right)\ll$$

$$\ll q^{-\nu r}\int_{(q\tau)^{-1}}^{\infty}z^{-\nu r}\,dz\ll q^{-1}P^{r-n-1},$$

$$F\ll\int_0^{P^{-n}}(q^{-1}P^{r-1}+q^{-2-\nu}P^{r+n-\nu}z)\,dz+$$

$$+\int_{P^{-n}}^{\infty}(q^{-1}z^{-\nu(r-1)}+q^{-2-\nu}z^{-\nu r+1}P^{n-\nu})\,dz\ll$$

$$\ll q^{-1}P^{r-n-1}+q^{-2-\nu}P^{r-n-\nu}.$$

因之,

$$H_{a,q}=R(N_0)\left(\frac{S_{a,q}}{q}\right)^r e^{-2\pi i\frac{a}{q}N_1}+O(q^{-1}P^{r-n-1}+q^{-2-\nu}P^{r-n-\nu}),$$

$$R(N_0)=\int_{-\infty}^{\infty}\psi^r e^{-2\pi izN_0}\,dz.$$

但若令 $M=\left[\frac{1}{2}P^{n-\nu}\right]$, 則有(運用第一章引理 3)

$$W(N_1)=H_{0,1}+\int_{\tau^{-1}}^{-\tau^{-1}+1}L_\alpha^r e^{-2\pi i\alpha N_1}\,d\alpha=$$

$$=R(N_0)+\int_{\tau^{-1}}^{-\tau^{-1}+1}L_\alpha^r e^{-2\pi i\alpha N_1}\,d\alpha+O(P^{r-n-\nu}),$$

$$\sum_{N'=1}^{M}\sum_{N''=1}^{M}W(N_0-N'-N'')=R(N_0)M^2+O\left(\int_{\tau^{-1}}^{-\tau^{-1}+1}P^r\frac{d\alpha}{(\alpha)^2}+P^{r-n-\nu}M^2\right),$$

$$M^2 r\nu T_r N_0^{r\nu-1}=R(N_0)M^2+O(P^{r-n-\nu}M^2),$$

$$R(N_0)=r\nu T_r N_0^{r\nu-1}+O(P^{r-n-\nu}),$$

$$H_{a,q}=r\nu T_r N_0^{r\nu-1}\left(\frac{S_{a,q}}{q}\right)^r e^{-2\pi i\frac{a}{q}N_1}+O(q^{-1}P^{r-n-1}+q^{-2-\nu}P^{r-n-\nu}).$$

將此不等式就所有與給定之 q 相應之 a, 然後再就所有之 $q=1,\cdots,[P^\beta]$ 求和, 並令 $N_1=N_0$, 則得

$$W_0(N_0)=F_r N_0^{r\nu-1}\sum_{0<q\leqslant P^\beta}A(q,N_0,r)+O(P^{r-n-\nu});\quad F_r=\frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu)}.\tag{3}$$

這公式也就是本章的目的.

第　四　章

華林問題中 $G(n)$ 的估值

在本章中, 當 $n\geqslant 3$ 時, 我們將解決華林問題, 此問題謂 (1770 年): 所有的正整數 N 皆可表成

$$N = x_1^n + \cdots + x_r^n \tag{1}$$

之形式,式中 $x_1, \cdots, x_r$ 爲非負整數, r 不超過一僅與 n 有關而與 N 無關的數目.

我們用記號 $G(n)$ 來表示具有這樣性質的 r 的最小數目:存在 $c = c(n)$, 使得所有 $\geqslant c$ 的整數 N 皆可表成 (1) 的形式,其 $r = G(n)$, 但決沒有 c' 使得所有 $\geqslant c'$ 的整數 N 皆可表成 (1) 的形式,其 $r < G(n)$. 如是, 則本章的結果可以更完全的寫成

$$G(n) < n(3\ln n + 11) \tag{2}$$

的形式.

這裏所用的方法也可以用來解決更普遍的問題;例如, 將充分大的整數 N 用多項式

$$a_n x^n + \cdots + a_2 x^2 + a_1 x$$

的值之和來表示的問題,這多項當其變數取整數值時取整數值,且不常爲某一大於 1 的數所除盡. 但我在這裏不來討論這種普遍性的問題.

爲了證明不等式 (2), 我現來討論一個定積分, 其與哈代-李托伍德在解決華林問題時所用的積分相似. 但在被積函數中,我引入了兩個因子(和數 Q_α 及 S_α), 使得可以按另外的方式來估計對應於餘區間的那一部分積分;詳言之,就是用由本書方法的一般考慮所得的估值去代替由外爾氏方法所得到的估值.

專用記號. 在本章中,我們將假定 $n \geqslant 3$, 並保持第三章中所用的記號 $r, N, c, P, \tau, \beta, L_\alpha, W_0(N_0)$, 且規定 $r = 4n$, $\beta = \frac{1}{4}$; 在該章中所說的將區間 $-\tau^{-1} \leqslant \alpha \leqslant -\tau^{-1} + 1$ 分成基本區間和餘區間的分法也仍然保留.

此外,設 $P_0 = [\sqrt{P}]$, v 跑過區間 $\frac{1}{2} P_0 \leqslant v \leqslant P_0$ 中之素數; V 是 v 的個數, 最後,設 u 與 u_0 跑過某些數值,關乎此,我們在後面將有所說明. 令

$$I(N) = \int_{-\tau^{-1}}^{-\tau^{-1}+1} L_\alpha^r Q_\alpha S_\alpha^2 e^{-2\pi i\alpha N} d\alpha; \; Q_\alpha = \sum_v \sum_{u_0} e^{2\pi i\alpha v^n u_0}; \; S_\alpha = \sum_u e^{2\pi i\alpha u};$$

$$k = \left[\frac{\ln 12n}{-\ln(1-\nu)} + 1\right]; \; k_0 = \left[\frac{\ln 6n}{-\ln(1-\nu)} + 2\right].$$

1. 數目 u 和數目 u_0. 設

$$P_1 = \left[\frac{1}{4}P\right]; \; P_2 = \left[\frac{1}{2}P_1^{1-\nu}\right]; \cdots, P_k = \left[\frac{1}{2}P_{k-1}^{1-\nu}\right].$$

令 ξ_s 跑過值 $\xi_s = P_s, \cdots, 2P_s - 1$. 任取一 $s = 1, \cdots, k$, 設

$$u_s = \xi_1^n + \cdots + \xi_s^n,$$

而來考慮由所有的 u_s 及數 $(2P_1)^n$ 所構成的集合 (u'_s).

運用歸納法不難證明,集合 (u'_s) 中之數總不出乎界限 P_1^n 與 $(2P_1)^n$ 之外,且互不相等. 同時,其中在數值上相隣的二數,其較大者與其較小者之差大於 nP_s^{n-1}.

事實上,我們的說法對於集合 (u'_1) 是對的,蓋其係由數

$$P_1^n, \cdots, (2P_1-1)^n, (2P_1)^n$$

所組成.

今設我們的說法對集合 (u'_s) 成立,並設 u' 與 u'' 爲此集合中在數值上相隣之二數. 我們來討論數

$$u', u'+P_{s+1}^n, \cdots, u'+(2P_{s+1}-1)^n, u''. \tag{3}$$

於此,我們有 (c 充分大)

$$(u'+P_{s+1}^n)-u' = P_{s+1}^n > nP_{s+1}^{n-1},$$

$$(u'+(\xi_{s+1}+1)^n)-(u'+\xi_{s+1}^n) > nP_{s+1}^n \, (\xi_{s+1} = P_{s+1}, \cdots, 2P_{s+1}-2),$$

$$u''-(u'+(2P_{s+1}-1)^n) > nP_s^{n-1}-(2P_{s+1})^n > nP_{s+1}^{n-1}.$$

此卽指出 (3) 中之數不出乎界限 u' 與 u'' 之外,且無兩者相等,同時,其中在數值上相隣之二數,其較大者與其較小者之差大於 nP_{s+1}^{n-1}. 因之,我們的說法對於集合 (u'_{s+1}) 也成立.

試注意 u_k 的個數等於

$$P_1 \cdots P_k \gg P^{1+(1-\nu)+\cdots+(1-\nu)^{k-1}} = P^{n-n(1-\nu)^k} \gg P^{n-\frac{1}{12}},$$

並令 $u = u_k$, 則基於上面所證,我們卽可斷定所有的 u 皆在區間 $(\frac{1}{5}P)^n < u < (\frac{1}{2}P)^n$ 中;這些數無兩者相等,且其中每一個皆是 k 個形如 ξ^n 的數之和,這裏的 ξ 是正整數;最後,對於這種數值的個數 U 我們有不等式

$$U \gg P^{n-\frac{1}{12}}.$$

重複類似的論證,但以 P_0 代 P, 以 k_0 代 k, 並注意

$$P_0^{n-n(1-\nu)k_0} \gg P_0^{n-\frac{1-\nu}{6}},$$

我們卽做成具有下述條件的數 u_0:

所有的 u_0 皆在區間 $(\frac{1}{5}P_0)^n < u_0 < (\frac{1}{2}P_0)^n$ 之內，其中無兩者相同，且每一個皆是形如 ξ_0^n 的 k_0 個數之和，此處的 ξ_0 是正整數；最後，對於這種數的個數 U_0，我們有不等式

$$U_0 \gg P_0^{n-\frac{1-\nu}{6}}.$$

2. 在餘區間上 Q_α 的估値. 依照第一章引理 7，區間 $-\tau^{-1} \leqslant \alpha \leqslant -\tau^{-1}+1$ 中所有的 α 皆可表成

$$\alpha = \frac{a}{q} + z;\ (a, q) = 1;\ 0 < q \leqslant \sqrt{N};\ |z| < \frac{1}{2\sqrt{N}} \tag{4}$$

的形式.

我們先就餘區間中能以 $q \leqslant P^{1/4}$ 表成 (4) 之形式的 α 來估計和數 Q_α. 此時，和數 Q_α 中，在給定的 $s = 0, \cdots, q-1$ 之下，對應於形如 $v = qt + s$ 的 v 的部分等於

$$\sum_{u_0} \sum_t e^{2\pi i u_0 \Phi(t)};\ \Phi(t) = \frac{as^n}{q} + z(qt+s)^n,$$

此處 t 跑過滿足條件

$$\frac{1}{2}P_0 \leqslant qt + s \leqslant P_0$$

的某些整數. 但隨 t 增到 1, $\Phi(t)$ 乃變爲某一形如 $nz(qt+q\theta+s)^{n-1}q$ 的數，其絕對值不出乎界限 A^{-1} 與 $2^{n-1}A^{-1}$ 之外，此處的 $A = 2^{n-1}(n|z|P_0^{n-1}q)^{-1}$. 同時，由於

$$\frac{1}{q\tau} \leqslant |z| \leqslant \frac{1}{q\sqrt{N}},$$

我們有 $P_0 \ll A \ll P_0^{n-1}$，因之，依照第一章引理 10，我們有

$$Q_\alpha \ll q\sqrt{U_0 \frac{P_0}{q} P_0^n} = U_0 P_0 \sqrt{\frac{P_0^n}{U_0} \frac{q}{P_0}} \ll U_0 V P_0^{\frac{1-\nu}{12}-\frac{1}{4}} \ln N.$$

現在，我們就餘區間中能以 $q > P^{\frac{1}{4}}$ 表成 (4) 之形式的 α 來估計和數 Q_α. 同餘式 $v^n \equiv y \pmod q$ 的解的個數 $\eta(y)$ 滿足條件

$$\eta(y) \leqslant \left(\frac{P_0}{q}+1\right) q^{\varepsilon};$$

故可令

$$Q_a = \sum_{u_0} \sum_{y} \eta(y)\, e^{2\pi i u_0 \frac{ay+\psi(y)}{q}};\ \psi(y) \ll 1.$$

運用第一章引理 10, b, 則得

$$Q_a \ll \sqrt{U_0\left(\frac{P_0}{q}+1\right) q^{\varepsilon} P_0 P_0^n} \ll U_0 P_0 \sqrt{\frac{P_0^n}{U_0}\left(\frac{1}{q}+\frac{1}{P_0}\right)} q^{\frac{\varepsilon}{2}} \ll$$

$$\ll U_0 V P_0^{\frac{1-\nu}{12}-\frac{1}{4}} N^{\varepsilon}.$$

3. $G(n)$ **的估值**. 我們現來估計積分 $I(N)$ 中對應於餘區間之部分 $I_1(N)$. 我們有

$$I_1(N) \ll P^r U_0 V P_0^{\frac{1-\nu}{12}-\frac{1}{4}} N^{\varepsilon} \int_0^1 |S_a|^2 d\alpha =$$

$$= P^r U_0 V P_0^{\frac{1-\nu}{12}-\frac{1}{4}} N^{\varepsilon} \int_0^1 \left(\sum_u \sum_{u'''} e^{2\pi i\alpha(u-u''')}\right) d\alpha,$$

此處的 u''' 跑過 u 所跑過的值. 由是

$$I_1(N) \ll P^r U_0 V P_0^{\frac{1-\nu}{12}-\frac{1}{4}} N^{\varepsilon} U \ll P^r U_0 V P^{\frac{1-\nu}{24}-\frac{1}{8}} N^{\varepsilon} P^{-n} U^2 P^{\frac{1}{12}} \ll$$

$$\ll P^{r-n} V U_0 U^2 P^{-\nu/25}.$$

我們再來估計積分 $I(N)$ 中對應於基本區間的部分 $I_0(N)$. 我們有

$$I_0(N) = \sum_{N_0} W_0(N_0);\ N_0 = N - u_0 v^n - u - u''',$$

$$N_0 > N - \left(\frac{1}{2}P_0\right)^n P_0^n - 2\left(\frac{1}{2}P\right)^n > \frac{1}{2}N.$$

由是,運用第三章公式 (3), 卽得

$$I_0(N) = F_r \sum_{N_0} N_0^{r\nu-1} \sum_{0<q\leqslant P^{\frac{1}{3}}} A(q, N_0, r) + O(V U_0 U^2 P^{r-n-\nu}).$$

再,我們有(第三章引理 6)

$$\sum_{q>P^{\frac{1}{3}}} A(q, N_0, r) \ll P^{-\frac{1}{3}},$$

因之,

$$I_0(N) = F_r \sum_{N_0} N_0^{r\nu-1} \mathfrak{S}(N_0, r) + O(V U_0 U^2 P^{r-n-\nu})$$

$$I(N) \gg V U_0 U^2 N^{r\nu-1}.$$

但 $I(N)$ 是將數 N 表成 $r+2k+k_0$ 個形如 w^n 的項之和的表示法的種數，此處 w 是正整數，而

$$r+2k+k_0 \leqslant \frac{2\ln 12n}{-\ln(1-\nu)}+\frac{\ln 6n}{-\ln(1-\nu)}+4+4n<$$

$$<\left(n-\frac{1}{2}\right)(2\ln 12n+\ln 6n)+4n+4<n(3\ln n+11).$$

故得

$$G(n)<n(3\ln n+11).$$

第 五 章

利用整多項式值的分數部分所作的近逼

在本章中，我將運用我的方法到這樣的問題，即利用整多項式值的分數部分來近逼所給定的眞分數的問題.

這裏所採用的方法，可能用來解決更廣泛的類似問題，例如對於那些就某種意義而言可以用整多項式去密切逼近的函數，我們用它的值底分數部分去近逼所給定的眞分數的問題. 但這類普遍性的問題我們在這裏不加討論。

專用記號. 在本章裏，我們假定 $n>4$，並採用下列記號:

$h,\cdots,j$ 及 n 是 g 個滿足條件 $0<h<\cdots<j<n$ 的整數；

$$f(x)=a_h x^h+\cdots+a_j x^j+a_n x^n;$$

$a_h,\cdots,a_j,a_n$ 爲實數，l 爲 $h,\cdots,j,n$ 中之一.

$$a_l=\frac{a}{q}+\frac{\theta}{q^2};\ (a,q)=1;\ q\geqslant c_0,$$

此處的 c_0 是一充分大的數,

$$\gamma=\frac{1}{g};\ \lambda=\frac{1}{l};\ D=h+\cdots+j+n;\ \rho=\frac{\gamma\lambda\nu}{4}\ \frac{\ln D}{(\ln D+1)\ln(D\ln D+D)};$$

$$k=\left[\frac{\ln(D\ln D+D)}{-\ln(1-\nu)}+1\right];\ p=q^{\lambda};\ p_t=p^{(1-\nu)^{t-1}};\ t=1,\cdots,k;$$

$$M=q^{\rho(1+\varepsilon_1)};\ \Delta=q^{-\rho};\ \kappa=\left[(k+1)\,g\,\varepsilon_1^{-1}+1\right];\ \sigma=(1-\nu)^k.$$

選取(這常是可能的) $c_1,\cdots,c_g$，使滿足條件

$$c_1 < \cdots < c_g, \quad \begin{vmatrix} c_1^{h-1} \cdots c_g^{h-1} \\ \cdots\cdots\cdots \\ c_1^{n-1} \cdots c_g^{n-1} \end{vmatrix} \neq 0,$$

並設

$$X_{t,s} = [p_t c_s]; \ \xi_t = [p_t^{1-\varepsilon}]; \ t = 1, \cdots, k; \ s = 1, \cdots, g,$$

我們用記號 $x_{t,s}$ 來記一變數,它跑過區間

$$X_{t,s} - \xi_t < x_{t,s} \leqslant X_{t,s} + \xi_t$$

中之整數;又用記號 G 來記數組 $(x_{1,1}, \cdots, x_{1,g}, \cdots, x_{k,1}, \cdots, x_{k,g})$ 的組數;顯而易見,

$$G = (2\xi_1)^g \cdots (2\xi_k)^g \gg (p_1 \cdots p_k)^{g(1-\varepsilon)}.$$

對每一 $t = 1, \cdots, k$, 取滿足條件 $0 < m_{t,s} < M$ 之任意整數 $m_{t,1}, \cdots, m_{t,g}$, 令

$$U_{t,r} = m_{t,1} x_{t,1}^r + \cdots + m_{t,g} x_{t,g}^r; \ U_r = U_{1,r} + \cdots + U_{k,r}; \ r = h, \cdots, j, n.$$

1. 一些方程組的解答個數的估計. 作一些長爲

$$Mp_t^{h-1}, \cdots, Mp_t^{n-1}$$

的區間,我們現來估計使 $U_{t,h}, \cdots, U_{t,n}$ 相應地落入這些區間的數組 $(x_{t,1}, \cdots, x_{t,g})$ 的組數 Φ_t'. 設 $(x_1, \cdots, x_g)$, $(x_1 + \zeta_1, \cdots, x_g + \zeta_g)$ 爲如是的二組. 則

$$m_{t,1}((x_1 + \zeta_1)^h - x_1^h) + \cdots + m_{t,g}((x_g + \zeta_g)^h - x_g^h) = \theta_h M p_t^{h-1},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$m_{t,1}((x_1 + \zeta_1)^n - x_1^n) + \cdots + m_{t,g}((x_g + \zeta_g)^n - x_g^n) = \theta_n M p_t^{n-1},$$

這可化爲

$$m_{t,1} c_1^{h-1} \beta_{h,1} \zeta_1 + \cdots + m_{t,g} c_g^{h-1} \beta_{h,g} \zeta_g = \theta_h M,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$m_{t,1} c_1^{n-1} \beta_{n,1} \zeta_1 + \cdots + m_{t,g} c_g^{n-1} \beta_{n,g} \zeta_g = \theta_n M,$$

在這裏,當 $c_0 = c_0(\varepsilon, n)$ 充分大時,所有的 $\beta_{r,s}$ 與 1 非常靠近,使得行列式

$$\begin{vmatrix} c_1^{h-1}\beta_{h,1}, \cdots, c_g^{h-1}\beta_{h,g} \\ \cdots\cdots\cdots\cdots\cdots \\ c_1^{n-1}\beta_{n,1}, \cdots, c_g^{n-1}\beta_{n,g} \end{vmatrix}$$

在數值上 $\gg 1$. 由是容易得出

$$m_{t,s}\zeta_s \ll M;\quad \zeta_s \ll \frac{M}{m_{t,s}};\quad s=1,\cdots,g.$$

因之,

$$\Phi_t' \ll \frac{M^g}{m_{t,1}\cdots m_{t,g}}.$$

再作一些長爲

$$Mp_t^{h(1-\nu)},\cdots,Mp_t^{n(1-\nu)}$$

的區間,我們現來估計使得 $U_{t,h},\cdots,U_{t,n}$ 分別落入這些區間的數組 $(x_{t,1},\cdots,x_{t,g})$ 的組數 Φ_t. 由

$$\frac{Mp_t^{h(1-\nu)}}{Mp_t^{h-1}}\cdots\frac{Mp_t^{n(1-\nu)}}{Mp_t^{n-1}} = p_t^{g-\nu D},$$

我們卽有

$$\Phi_t \ll \frac{M^g p_t^{g-\nu D}}{m_{t,1}\cdots m_{t,g}}.$$

對於數 $U_{t,r}$, 我們也有不等式

$$U_{t,r} \ll Mp_t^r.$$

對於方程組

$$U_h = z_h,\cdots,U_n = z_n$$

的解的組數 $\psi_0(z_h,\cdots,z_n)$, 依照第一章引理 15, 我們有

$$\psi_0(z_h,\cdots,z_n) \ll \Phi_1\cdots\Phi_k \ll \Phi;\ \Phi = \frac{M^{gk}(p_1\cdots p_k)^{g-\nu D}}{m_{1,1}\cdots m_{1,g}\cdots m_{k,1}\cdots m_{k,g}}. \tag{1}$$

對於數 U_r, 我們也有不等式

$$U_r \ll Mp^r. \tag{2}$$

2. 基本和數的估値. 我們現來估計和數

$$T = \sum_{y=1}^{p}\left|\sum\nolimits_0 e^{2\pi i(a_h y^h U_h+\cdots+a_n y^n U_n)}\right|,$$

於此, Σ_0 係表一和數,其求和範圍係展佈於所有的 G 個數組 $(x_{1,1},\cdots,x_{1,g},\cdots,x_{k,1},\cdots,x_{k,g})$, 也就是展佈於所有的 G 個數組 $(U_h,\cdots,U_n)$. 我們有

$$|T|^2 \ll p\sum_{y=1}^{p}\sum\nolimits_0'\sum\nolimits_0 e^{2\pi i(a_h y^h(U_h'-U_h)+\cdots+a_n y^n(U_n'-U_n))},$$

這裏的數組（$U_h', \cdots, U_n'$）是和數組（$U_h, \cdots, U_n$）處於同樣情形.

用記號 $\psi(u_h, \cdots, u_n)$ 記不定方程組

$$U_h' - U_h = u_h, \cdots, U_n' - U_n = u_n \tag{3}$$

的解的組數，由（1），顯然有

$$\psi(u_h, \cdots, u_n) \ll G\Phi.$$

由（2），存在數 $c^{(h)}, \cdots, c^{(n)}$，使得不定方程組（3）僅對於屬於區間

$$-c^{(h)} M p^h \leqslant u_h \leqslant c^{(h)} M p^h, \cdots, -c^{(n)} M p^n \leqslant u_n \leqslant c^{(n)} M p^n$$

中的 $u_h, \cdots, u_n$ 始有可能成立. 令 $u_h, \cdots, u_n$ 跑過這些區間中的整數，則得

$$\sum_{u_h} \cdots \sum_{u_n} (\psi(u_h, \cdots, u_n))^2 \ll G\Phi \sum_{u_h} \cdots \sum_{u_n} \psi(u_h, \cdots, u_n) = G^3\Phi.$$

由上所述，我們有（參看第一章引理 10, b 的證明）

$$|T|^2 \leqslant p \sum_{u_h} \cdots \sum_{u_n} \psi(u_h, \cdots, u_n) \sum_{y=1}^{p} e^{2\pi i(a_h y^h u_h + \cdots + a_n y^n u_n)},$$

$$T^4 \ll \frac{p^2 G^3 \Phi}{M p^l} \sum_{u_h} \cdots \sum_{u_l'} \sum_{u_l} \cdots \sum_{u_n} \left| \sum_{y=1}^{p} e^{2\pi i(a_h y^h u_h + \cdots + a_l y^l (u_l' + u_l) + \cdots + a_n y^n u_n)} \right|^2,$$

這裏引進來了一個補充變數 u_l'，它跑過區間

$$-2c^{(l)} M p^l \leqslant u_l' \leqslant 2c^{(l)} M p^l$$

中的整數. 由是卽得

$$T^4 \ll p^2 G^3 \Phi M^{-1} p^{-l} M^{g-1} p^{D-l} \sum_{y_1=1}^{p} \sum_{y=1}^{p} \left| \sum_{u_l'} \sum_{u_l} e^{2\pi i a_l (y_1^l - y^l)(u_l' + u_l)} \right| \ll$$

$$\ll G^3 \Phi M^{g-2} p^{D-2l+2} \sum_{y_1=1}^{p} \sum_{y=1}^{p} \min\left(M^2 p^{2l}, \frac{1}{4(a_l(y_1^l - y^l)^2)}\right).$$

當 y_1 給定時，差數 $y_1^l - y^l$ 跑過了屬於長爲 q 的某區間中的一些整數. 故由第一章引理 8, a, 我們有

$$T^4 \ll G^3 \Phi M^{g-2} p^{D-2l+2} p(M^2 p^{2l} + M p^l q) \ll G^3 \Phi M^g p^{D+3},$$

$$\frac{T}{pG} \ll (G^{-1} \Phi M^g p^{D-1})^{1/4} \ll \left(\frac{M^{g(k+1)} (p_1 \cdots p_k)^{-\nu D + g\varepsilon} p^{D-1}}{m_{1,1} \cdots m_{1,g} \cdots m_{k,1} \cdots m_{k,g}}\right)^{1/4},$$

$$T \ll p\,G\,\frac{q^{\frac{\rho g(k+1)}{4}-\frac{\lambda}{4}+\frac{\lambda\sigma D}{4}+\varepsilon'}}{(m_{1,1}\cdots m_{1,g}\cdots m_{k,1}\cdots m_{k,g})^{1/4}}.$$

定理. 存在 $c=c(n)$，使得對於任意實數 A，不等式組

$$|f(x)-v-A|<cq^{-\rho};\ 0<x<q^{2\lambda}$$

可爲整數 x 及 v 所滿足.

證. 由第一章引理 12，存在函數 $\psi(x)$，其週期爲 1，且具有下之性質 $(\alpha+\frac{1}{2}\Delta=A=\beta-\frac{1}{2}\Delta)$

1. $0\leqslant\psi(x)\leqslant 1$，在區間 $A-\Delta\leqslant x\leqslant A+\Delta$ 內.
2. $\psi(x)=0$，在區間 $A+\Delta\leqslant x\leqslant 1+A-\Delta$ 內.
3. $\psi(x)$ 可展成形如

$$\psi(x)=\Delta+\psi_0(x),\ \psi_0(x)=\sum_{m=1}^{\infty}(A_m\cos 2\pi mx+B_m\sin 2\pi mx)$$

之富理級數，此處 $A_m\ll F(m)$，$B_m\ll F(m)$，且

$$F(m)=\begin{cases}\Delta, 若\ m\leqslant\frac{1}{\Delta},\\ \frac{1}{\Delta^{\kappa}m^{\kappa+1}}, 若\ m>\frac{1}{\Delta}.\end{cases}$$

我們現來討論和數

$$H=\sum_{y=1}^{p}\left|\sum_{x_{1,1}}\psi_0(f(yx_{1,1}))\cdots\sum_{x_{1,g}}\psi_0(f(yx_{1,g}))\cdots\right.$$
$$\left.\cdots\sum_{x_{k,1}}\psi_0(f(yx_{k,1}))\cdots\sum_{x_{k,g}}\psi_0(f(yx_{k,g}))\right|.$$

於此，我們有

$$\sum_{x_{t,s}}\psi_0(f(yx_{t,s}))\ll\sum_{m_{t,s}=1}^{\infty}F(m_{t,s})\left|\sum_{x_{t,s}}e^{2\pi i m_{t,s}f(yx_{t,s})}\right|.$$

故得

$$H\ll\sum_{m_{1,1}=1}^{\infty}\cdots\sum_{m_{1,g}=1}^{\infty}\cdots\sum_{m_{k,1}=1}^{\infty}\cdots\sum_{m_{k,g}=1}^{\infty}F(m_{1,1})\cdots$$
$$\cdots F(m_{1,g})\cdots F(m_{k,1})\cdots F(m_{k,g})\,T,$$

此處的 T 是在第二段中所討論過的和數. 由

$$\sum_{m=1}^{\infty} F(m) \ll 1;\ \sum_{m\leqslant M} \frac{F(m)}{m^{1/4}} \ll \Delta M^{3/4};\ \sum_{m>M} F(m) \ll \frac{1}{\Delta^{\kappa} M^{\kappa}} \ll q^{-\rho g(k+1)},$$

和數 H 的被加項中,其至少有一 $m_{t,s}$ 超過 M 者，其和將

$$\ll p\, G\, q^{-\rho g(k+1)} = p\, \Delta^{gk}\, G\, q^{-\rho g};$$

而和數 H 中留來的各項之和將

$$\ll p\, G\, q^{\frac{\rho g(k+1)}{4} - \frac{\lambda}{4} + \frac{\lambda\sigma D}{4} + \frac{3\rho g k}{4} + \varepsilon''}\, \Delta^{gk} \ll pG\Delta^{gk}\, q^{\rho g(k+\frac{1}{4}) - \frac{\lambda}{4} + \frac{\lambda\sigma D}{4} + \varepsilon''}.$$

但這裏 q 的指數將

$$< \frac{\lambda \ln D\left(\left(1-\frac{v}{2}\right)\ln(D\ln D+D)+\frac{5}{4}v\right)}{4(\ln D+1)\ln(D\ln D+D)} - \frac{\lambda}{4} + \frac{\lambda}{4(\ln D+1)} < 0.$$

因之，對於某兩數 c_1 與 c''',

$$H < p\, G\, c_1^{gk}\, \Delta^{gk}\, q^{-c'''gk};\ \sum_{y=1}^{p} \prod_{\substack{t=1,\cdots,k\\ s=1,\cdots,g}} \frac{\left|\sum_{x_{t,s}} \psi_0(f(yx_{t,s}))\right|}{\Delta G_{t,s}} < pc_1^{gk}\, q^{-c'''gk}.$$

故知至少必有一組值 y, t, s 存在,使得

$$\frac{\left|\sum_{x_{t,s}} \psi_0(f(yx_{t,s})\right|}{\Delta G_{t,s}} < c_1\, q^{-c'''}.$$

我們可將數 c_0 取得充分大,使此不等式之右邊 <1, 由此卽可推出,對於某一 $x=x_{t,s}$,

$$\psi_0(f(yx)) < \Delta;\ \psi(f(yx)) > 0,$$

我們的定理由是卽已證明.

例. 設 α 爲實數,

$$f(x) = \alpha x^n + x\sqrt{2};\ n > 4;\ \tau \geqslant 1.$$

將 $\sqrt{2}$ 展成連分數,我們現來討論其漸近分數中,分母 q 與 q' 滿足條件 $q \leqslant \sqrt{\tau} < < q'$ 的那一對相隣的漸近分數. 由於部分商有界，$q' \ll q$，故由定理卽可斷定有整數 z 及 v 滿足不等式組

$$|f(z) - v - A| \leqslant c\,\tau^{-\rho_0};\qquad 0 < z < \tau,$$

$$\rho_0 = \frac{\ln(n+1)}{8n(\ln(n+1)+1)\ln((n+1)\ln(n+1)+n+1)}.$$

第 六 章

外爾和數的估值

在本章裏,我將運用我的方法去導出兩個可以用來估計形如

$$\sum_{x=M}^{M+P-1} e^{2\pi i f(x)}$$

的和數的普遍性定理,這裏的 $f(x)$ 可以是 $n+1$ 次整多項式(此時估值取決於 x 之高於一次方的係數之有理近逼),也可以是依某種意義而言能以 n 次整多項式密切逼近的函數.

這一方法也適用於數目 n 隨函數 $f(x)$ 之形狀及求和區間的變化而同時增長的情形. 但此種情形我們在這裏不加討論.

專用記號. 在本章中,我們將假定 $n \geqslant 11$,用字母 k 表示一個大於 n 然而不大於某一常數的整數,又設

$$\sigma = (1-\nu)^k;\quad h = n+2;\quad b = \left[\frac{5}{4}n + \frac{1}{2}\right].$$

引理. 設 p_1 爲整數, $p_1 > c_0$, 此處 c_0 爲一充分大的數;

$$p_t = p_1^{(1-\nu)^{t-1}},\quad \eta_t = [\nu \ln_2 p_t] \qquad (t=1,\cdots,k+1),$$

$a_{n+1},\cdots,a_1$ 爲實數, $f(x) = a_{n+1}x^{n+1} + \cdots + a_1 x$;

$$T_1 = \sum_{x=1}^{p_1} e^{2\pi i f(x)}.$$

則有

$$T_1^{2b(k+h)} \ll \sum_{s_1=2}^{\eta_1} \cdots \sum_{s_k=2}^{\eta_k} \sum^{B} K(s_1,\cdots,s_k),$$

$$B = p_1^{2b(k+h)}(p_1\cdots p_k)^{-2b} p_{k+1}^{-2bh} 2^{(2n-2h(b-n))(s_1+\cdots+s_k)}, \tag{1}$$

$$K(s_1,\cdots,s_k) = \sum_{(x_1,\cdots,x_{n+1})} e^{2\pi i(X_1x_1+\cdots+X_{n+1}x_{n+1})};\quad X_r = \frac{f^{(r)}(x_0)}{r!},$$

此處的 x_0 是整數. 多項式 $X_1,\cdots,X_{n+1}$ 的 x_0 各次冪的係數僅與 $a_{n+1},\cdots,a_1$ 有關. 求和範圍係展布於由屬於形如

$$-cp_1 \leqslant x_1 \leqslant cp_1, \cdots, -cp_1^{n+1} \leqslant x_{n+1} \leqslant cp_1^{n+1}$$

的區間中之整數所組成的數組 $(x_1, \cdots, x_{n+1})$，而無論任何整數 $z_1, \cdots, z_n$，數組 $(x_1, \cdots, x_{n+1})$ 中，其滿足條件

$$x_1 = z_1, \cdots, x_n = z_n$$

者，爲數將

$$\ll \psi; \quad \psi = (p_1 \cdots p_k)^{2b - \frac{n+1}{2}} p_{k+1}^{2bh} \, 2^{\left(-2b + \frac{n(n+1)}{2}\right)(s_1 + \cdots + s_k)}.$$

因而

$$B\psi \ll p_1^{2b(k+h) - \frac{n(n+1)}{2} + \frac{n(n+1)}{2}\sigma} \, 2^{-4(s_1 + \cdots + s_k)}.$$

證. 令 $R_{t,s} = p_t 2^{-s}$. 對 $t = 1, \cdots, k+1$，我們用記號 T_t 來記所有形如

$$T_t = \sum e^{2\pi i f(x)}$$

之和，這裏的 x 跑過數列 $1, \cdots, p_1$ 中，任何 $\leqslant p_t$ 個相繼的數. 任取數列 $1, \cdots, \eta_t$ 中之一數 s，我們將和數 T_t 之求和區間分成形如 (ω_t 與 s 無關)

$$\omega_t + (g-1) R_{t,s} < x \leqslant \omega_t + (g-1) R_{t,s} + R'_{t,s}, \tag{2}$$

$$(g = 1, \cdots, g'; \quad g' \leqslant 2^s, R'_{t,s} \leqslant R_{t,s})$$

之區間. 由是 T_t^b 卽被分成 $\leqslant 2^{sb}$ 個積 $Z_{t,s}$ 之和

$$T_t^b = \sum Z_{t,s}; \quad Z_{t,s} = Z_{t,s,1} \cdots Z_{t,s,b}; \quad Z_{t,s,j} = \sum_x e^{2\pi i f(x)}.$$

在這裏，$Z_{t,s,j}$ 之求和區間乃是 (2) 中之一區間；與這區間相應的值 g 稱爲 $Z_{t,s,j}$ 之編號.

若在所有 $Z_{t,s,j}$ 的編號中，有着 n 個這樣的編號，其中任何兩個的差皆 > 1 者，則 $Z_{t,s}$ 稱爲規則的；不然則稱 $Z_{t,s}$ 爲不規則的.

設 g_1 爲不規則的 $Z_{t,s}$ 之諸因子 $Z_{t,s,j}$ 的編號中最小者；g_2 爲此種編號中超過 g_1+1 的最小者；g_3 爲超過 g_2+1 之編號中的最小者等等；最後，設 g_{n_1} 爲超過 $g_{n_1-1}+1$ 之編號中的最小者，而超過 $g_{n_1}+1$ 之編號則無有. 顯而易見，$n_1 < n$ (否則 $Z_{t,s}$ 將爲規則的). 令 $g'_1, \cdots, g'_{n-1}$ 互相獨立的跑過值 $1, \cdots, 2^s$，我們卽得 $2^{s(n-1)}$ 個數組 $g'_1, \cdots, g'_{n-1}$；於其中找出包含所有數目 $g_1, \cdots, g_{n_1}$ 的數組，而由後者

的構成方法，即可推知所有 $Z_{t,s,j}$ 的編號皆可於數目

$$g_1',\ g_1'+1,\ g_2',\ g_2'+1,\cdots,\ g_{n-1}',\ g_{n-1}'+1 \tag{3}$$

中找到．令 $g_1'',\cdots,g_b''$ 相互獨立的跑過數列 (3)，我們即得 $(2n-2)^b$ 個數組 $g_1'',\cdots,g_b''$；於其中找出由所論的 $Z_{t,s}$ 之諸因子 $Z_{t,s,j}$ 的編號所構成的數組．由所說即可推知，不規則的 $Z_{t,s}$ 的數目 $B_{t,s}$ 滿足不等式

$$B_{t,s}\leqslant 2^{s(n-1)}(2n-2)^b.$$

由區間 (2) 的構成方法即可推知，當 $s=2,\cdots,n$ 時，每一不規則的 $Z_{t,s-1}$ 皆可表成 $\leqslant 2^b$ 個乘積 $Z_{t,s}$ 之和．對於異於 η_t 之 s，我們用記號 $Z'_{t,s}$ 來記其中之規則乘積；而當 $s=\eta_t$ 時，其所有之乘積皆以 $Z'_{t,s}$ 記之．顯而易見，乘積 $Z'_{t,s}$ 之總數

$$\leqslant B_{t,s-1}2^b\ll 2^{-s}2^{sn}.$$

當 $t=1,\cdots,k$，我們有（第一章引理 2 及 1,b）

$$T_t^b=\sum_{s=2}^{\eta_t}2^{-s}\sum^{2^{sn}}Z'_{t,s};\quad T_t^{2b(k-t+h+1)}\ll\sum_{s=2}^{\eta_t}\left(\sum^{2^{sn}}|Z'_{t,s}|\right)^{2(k-t+h+1)}\ll$$

$$\ll\sum_{s=2}^{\eta_t}2^{sn(2(k-t+h+1)-1)}\sum^{2^{sn}}|Z'_{t,s}|^{2(k-t+h+1)}\ll$$

$$\ll\sum_{s=2}^{\eta_t}\sum^{2^{2sn(k-t+h+1)}}|Z'_{t,s}|^2\,|Z'_{t,s}|^{2(k-t+h)},$$

$$b^b|Z'_{t,s}|\ll\left(\sum_{j=1}^{b}|Z_{t,s,j}|\right)^b;\quad |Z'_{t,s}|^{2(k-t+h)}\ll\left(\sum_{j=1}^{b}|Z_{t,s,j}|\right)^{2b(k-t+h)}.$$

但每一 $Z_{t,s,j}$ 皆可分成

$$\leqslant p_t 2^{-s}p_{t+1}^{-1}+1=p_t^{\nu}2^{-s}(1+2^s p_t^{-\nu})\leqslant 2p_t^{\nu}2^{-s}$$

個和數 T_{t+1}；因之

$$\sum_{j=1}^{b}|Z_{t,s,j}|^{2b(k-t+h)}\ll\sum_{j=1}^{b}(p_t^{\nu}2^{-s})^{(2b(k-t+h)-1)}\sum^{p_t^{\nu}2^{-s}}|T_{t+1}|^{2b(k-t+h)}\ll$$

$$\ll\sum^{(p_t^{\nu}2^{-s})^{2b(k-t+h)}}|T_{t+1}|^{2b(k-t+h)},$$

$$T_t^{2b(k-t+h+1)} \ll \sum_{s=2}^{\eta_t} \sum^{M_{t,s}} |Z'_{t,s}|^2 |T_{t+1}|^{2b(k-t+h)},$$

$$M_{t,s} = 2^{-s(2b-2n)(k-t+h)+2sn} p_t^{2b\nu(k-t+h)}.$$

在這公式裏寫 s_t 代 s, 並將其運用於 $t=1, \cdots, k$. 注意

$$k-t+h \geqslant h; \quad p_t^{\nu} = \frac{p_t}{p_{t+1}},$$

$$\left(\frac{p_1}{p_2}\right)^{k+h-1}\left(\frac{p_2}{p_3}\right)^{k+h-2}\cdots\left(\frac{p_k}{p_{k+1}}\right)^{k+h-k} = p_1^{k+h}(p_1\cdots p_k)^{-1}p_{k+1}^{-h},$$

我們卽得公式 (1),其中之 B 有如定理之陳述中所說,但

$$K(s_1, \cdots, s_k) = |Z'_{1,s_1}|^2 \cdots |Z'_{k,s_k}|^2 |T_{k+1}|^{2bh}.$$

我們現來研究任意一個固定的 $K(s_1, \cdots, s_k)$. 設 $e^{2\pi i f(x_0)}$ 爲和數 T_{k+1} 的一項. 乘積 Z'_{t,s_t} 的因子 $Z_{t,s_t,j}$ 可以表成形如

$$\sum_{v_t} e^{2\pi i\left(X_0+X_1 v_t+\cdots+X_{n+1}v_t^{n+1}\right)}$$

之和數,這裏的 v_t 跑過數目 $x-x_0$ (x 跑過 $Z_{t,s_t,j}$ 之求和區間內的整數), $X_0=f(x_0)$, 而 $X_1, \cdots, X_{n+1}$ 則具有引理的陳述中所說的值. 設 $s_t<\eta_t$, 又設 $g_1, \cdots, g_n$ 是 $Z'_{,t_s}$ 的因子 $Z_{t,s_t,j}$ 中可以表明它是規則乘積的那種因子的編號, 而按從小到大的次序排列者. 我們分別用 $v_{t,s_t,1}, \cdots, v_{t,s_t,n}$ 來記這些因子的求和變數;同時,對 $r=1, \cdots, n+1$, 我們令

$$V_{t,s_t,r} = v^r_{t,s_t,1} + \cdots + v^r_{t,s_t,n}.$$

則 $|Z'_{t,t_s}|^2$ 可以表成和數

$$\sum_{(V_{t,s_t,1},\cdots,V_{t,s_t,n+1})} \sum_{(W_{t,s_t,1},\cdots,W_{t,s_t,n+1})} e^{2\pi i\left(X_1\left(V_{t,s_t,1}+W_{t,s_t,1}\right)+\cdots+X_{n+1}\left(V_{t,s_t,n+1}+W_{t,s_t,n+1}\right)\right)},$$

此處的第二求和記號與第一個無關,它展布於 $\ll R_{t,s_t}^{2b-n}$ 個由滿足條件 $W_{t,s_t,r} \ll p_t^r$ 之整數所組成的數組 $(W_{t,s_t,1}, \cdots, W_{t,s_t,n+1})$ 之上. 數組 $(V_{t,s_t,1}, \cdots, V_{t,s_t,n+1})$ 中之數滿足條件 $V_{t,s_t,r} \ll p_t^r$, 而且 (第一章引理 16, 置 $p=p_t$, $R=R_{t,s_t}$, $H=2^{s_t}$) 無論對於任何長爲

$$p_t^{1-\nu}, \cdots, p_t^{n(1-\nu)} \tag{4}$$

之區間,數組 $(V_{t,s_t,1}, \cdots, V_{t,s_t,n+1})$ 中,其數 $V_{t,s_t,1}, \cdots, V_{t,s_t,n}$ 分别落入這些區間者,爲數將

$$\ll 2^{s_t \frac{n(n-1)}{2}} p_t^{\frac{n-1}{2}}.$$

令 $U_{t,s_t,r} = V_{t,s_t,r} + W_{t,s_t,r}$, 則我們卽已證明

$$|Z'_{t,s_t}|^2 = \sum_{(U_{t,s_t,1},\cdots,U_{t,s_t,n+1})} e^{2\pi i\left(X_1 U_{t,s_t,1} + \cdots + X_{n+1} U_{t,s_t,n+1}\right)},$$

這裏的求和記號係展布於由滿足條件 $U_{t,s_t,r} \ll p_t^r$ 之整數所組成的數組 $(U_{t,s_t,1}, \cdots, U_{t,s_t,n+1})$ 之上,而且,無論任何長爲 (4) 之區間,這種數組中,其數 $U_{t,s_t,1}, \cdots, U_{t,s_t,n}$ 分别落入所說之區間者,爲數將

$$\ll \Phi_{t,s_t}; \quad \Phi_{t,s_t} = p_t^{2b-\frac{n+1}{2}} 2^{\left(-2b+\frac{n(n+1)}{2}\right)s_t}.$$

這項估値當 $s_t = \eta_t$ 時也成立,因爲所有數組 $(U_{t,\eta_t,1}, \cdots, U_{t,\eta_t,n+1})$ 的數目將

$$\ll p_t^{2b} 2^{-2b\eta_t} \ll p_t^{2b} 2^{2b\eta_t} p_t^{-\frac{n+1}{2}} 2^{\frac{n(n+1)}{2}\eta_t} = \Phi_{t,\eta_t}.$$

注意 $|T_{k+1}|^{2bh}$ 可以表成 $\ll p_{k+1}^{2bh}$ 項形如

$$e^{2\pi i\left(X_1 x_1' + \cdots + X_{n+1} x_{n+1}'\right)}$$

的項之和,這裏的 $x_1', \cdots, x_{n+1}'$ 是滿足條件 $x_r' \ll p_1^r$ 的整數,則我們卽已證明 $K(s_1, \cdots, s_k)$ 眞正可以表成如在引理的陳述中所說形狀的和數,其中

$$x_r = U_r + x_r'; \quad U_r = U_{1,s_1,r} + \cdots + U_{k,s_k,r};$$

而且,對於某一 c, 在引理中所說的關於 $x_1, \cdots, x_{n+1}$ 之不等式也成立. 又運用第一章引理 15 (假定 $h, \cdots, l$ 就是全部的數目 $1, 2, \cdots, n-1$), 則卽已證明數組 $(x_1, \cdots, x_{n+1})$ 中,其滿足條件 $x_1 = z_1, \cdots, x_{n+1} = z_{n+1}$ 者,爲數將

$$\ll \Phi_{1,s_1} \cdots \Phi_{k,s_k} p_{k+1}^{2bh} \ll \psi.$$

在引理中所說的關於 $B\psi$ 之不等式易於得出.

定理 1. 設 m 與 P 爲正整數;

$$S = \sum_{x=1}^{P} e^{2\pi i m F(x)}, \quad F(x) = a_{n+1} x^{n+1} + \cdots + a_1 x;$$

$a_{n+1}, \cdots, a_1$ 爲實數；r 爲 $n+1, \cdots, 2$ 中之一；

$$a_r = \frac{a}{q} + \frac{\theta}{q^2};\quad (a, q) = 1;\quad q > 0.$$

則有

$$S \ll P^{1-\rho t} m^{2\rho r-1};\quad \rho = \frac{\tau}{3n^2 \ln \frac{12\,n(n+1)}{\tau}};\quad t = 1 + \frac{\nu}{30},$$

於此，對於預先給定的 c_1 和 c_2（例如可取 $c_1 = c_2 = 1$），τ 係由下之等式所定義

1. $q = c_1 P^\tau$　，　若　$1 < q \leqslant c_1 P$，
2. $\tau = 1$　，　若　$c_1 P \leqslant q \leqslant c_2 P^{r-1}$，
3. $q = c_2 P^{r-\tau}$　，　若　$c_2 P^{r-1} \leqslant q < c_2 P^r$，

且服從條件 $\tau \geqslant \tau_0$，此處的 τ_0 爲一正常數（任意小）.

證．設

$$Y = [P^{1-\rho t}],\quad k = \left[\frac{\ln \frac{3n(n+1)}{\tau}}{-\ln(1-\nu)} + 1\right].$$

則易得出

$$(n-1)\ln\frac{3n(n+1)}{\tau} < k < \left(n - \frac{1}{2}\right)\ln\frac{3n(n+1)}{\tau} + 1,$$

$$\sigma < \frac{\tau}{3n(n+1)}.$$

對 $y = 0, \cdots, Y-1$，置

$$T_0 = \sum_{x=1}^{P} e^{2\pi i(mF(y+x) - mF(y))},$$

則有

$$|S| = |T_0| + 2\theta y;\quad |S| = Y^{-1}\sum_{y=0}^{Y-1} |T_0| + \theta' Y.$$

由是即得（第一章引理 1, b）

$$|S|^{2b(k+h)} \ll \left(Y^{-1}\sum_{y=0}^{Y-1} |T_0|\right)^{2b(k+h)} + Y^{2b(k+h)} \ll$$

$$\ll Y^{-1}\sum_{y=0}^{Y-1} |T_0|^{2b(k+h)} + Y^{2b(k+h)}.$$

運用戴勞公式，即得

$$mF(y+x)-mF(y)=Y_1 x+\cdots+Y_{n+1}x^{n+1},$$

$$Y_j=Y_j(y)=\frac{mF^{(j)}(y)}{j!}=\binom{n+1}{j}ma_{n+1}y^{n+1-j}+\cdots+\binom{j+1}{j}ma_{j+1}y+ma_j.$$

再令

$$T_1=\sum_{x=1}^{P}e^{2\pi i\left(a_1x+\cdots+a_nx^n+ma_{n+1}x^{n+1}\right)}.$$

若點 $(\alpha_1,\cdots,\alpha_n)$ 屬於 n 次元空間中由不等式

$$Y_1-\frac{1}{2}P^{-1-\rho t}\leqslant\alpha_1\leqslant Y_1+\frac{1}{2}P^{-1-\rho t},\cdots,$$

$$Y_n-\frac{1}{2}P^{-n-\rho t}\leqslant\alpha_n\leqslant Y_n+\frac{1}{2}P^{-n-\rho t}$$

所定義之域 (Ω_y),則有

$$T_0=T_1+O(Y);\quad |T_0|^{2b(k+h)}\ll|T_1|^{2b(k+h)}+Y^{2b(k+h)}.$$

將上之不等式兩邊乘以

$$P^{\frac{n(n+1)}{2}+n\rho t}\,d\alpha_1\cdots d\alpha_n$$

並在域 (Ω_y) 上求積分,卽得

$$|T_0|^{2b(k+h)}\ll P^{\frac{n(n+1)}{2}+n\rho t}\int_{(\Omega y)}\!\!\cdots\!\int|T_1|^{2b(k+h)}d\alpha_1\cdots d\alpha_n+Y^{2b(k+h)},$$

$$S^{2b(k+h)}\ll P^{\frac{n(n+1)}{2}-1+(n+1)\rho t}\sum_{y=0}^{Y-1}\int_{(\Omega y)}\!\!\cdots\!\int|T_1|^{2b(k+h)}d\alpha_1\cdots d\alpha_n+Y^{2b(k+h)}.\qquad(5)$$

設 $(\alpha_1,\cdots,\alpha_n)$ 爲一旣定的點,我們現來估計那種域 (Ω_y) 的數目 G,它包含有一點,其位標與 $(\alpha_1,\cdots,\alpha_n)$ 之位標僅在整數部分不同者. 設 (Ω_y) 與 (Ω_{y_0}) 爲兩個這樣的域. 若用 $C_1,C_2,\cdots$ 來記某些整數,則有

$$Y_{r-1}(y)-Y_{r-1}(y_0)=C_{r-1}+O(P^{-r+1-\rho t}),\cdots,$$
$$Y_n(y)-Y_n(y_0)=C_n+O(P^{-n-\rho t}).$$

這可依相反的次序寫成:

$$C_n+O(P^{-n-\rho t})=\binom{n+1}{n}ma_{n+1}(y-y_0),$$

$$C_{n-1}+O(P^{-n+1-\rho t})=\binom{n+1}{n-1}ma_{n+1}(y^2-y_0^2)+\binom{n}{n-1}ma_n(y-y_0),$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$C_{r-1}+O(P^{-r+1-\rho t})=\binom{n+1}{r-1}ma_{n+1}(y^{n+2-r}-y_0^{n+2-r})+\cdots+\binom{r}{r-1}ma_r(y-y_0).$$

將這些等式逐項乘以

$$D_n=1!;\quad D_{n-1}=1!\,2!;\cdots;\quad D_{r-1}=1!\,2!\cdots(n+2-r)!,$$

我們卽得下之等式:

$$C'_n+O(P^{-n-\rho t})=D_n\binom{n+1}{n}ma_{n+1}(y-y_0),$$

$$C'_{n-1}+O(P^{-n+1-\rho t})=D_{n-1}\binom{n+1}{n-1}ma_{n+1}(y^2-y_0^2)+D_{n-1}\binom{n}{n-1}ma_n(y-y_0),$$

....

$$C'_{r-1}+O(P^{-r-1-\rho t})=D_{r-1}\binom{n+1}{r-1}ma_{n+1}(y^{n+2-r}-y_0^{n+2-r})+\cdots+$$

$$+D_{r-1}\binom{r}{r-1}ma_r(y-y_0).$$

第一等式的右邊可以除盡所有其餘各等式右邊的第一項,除得的商分別爲

$$\ll P,\cdots,\ll P^{n+1-r}.$$

用第一等式的左邊乘這些商數所得的積各與某一整數之差分別爲

$$\ll P^{-n+1-\rho t},\cdots,\ll P^{-r+1-\rho t}.$$

故其餘各等式可以化成

$$C''_{n-1}+O(P^{-n+1-\rho t})=D_{n-1}\binom{n}{n-1}ma_n(y-y_0),$$

....

$$C''_{r-1}+O(P^{-r+1-\rho t})=D_{r-1}\binom{n}{r-1}ma_n(y^{n+1-r}-y_0^{n+1-r})+\cdots+$$

$$+D_{r-1}\binom{r}{r-1}ma_r(y-y_0).$$

運用與上述相類似的討論於這些等式,我們卽得新等式

$$C'''_{n-2}+O(P^{-n+2-\rho t})=D_{n-2}\binom{n-1}{n-2}ma_{n-1}(y-y_0),$$

....

$$C'''_{r-1}+O(P^{-r+1-\rho t})=D_{r-1}\binom{n-1}{r-1}ma_{n-1}(y^{n-r}-y_0^{n-r})+\cdots+D_{r-1}\binom{r}{r-1}ma_r(y-y_0)$$

等等. 最後,我們得到一個形如

$$C + O(P^{-r+1-\rho t}) = D_{r-1}\binom{r}{r-1} ma_r (y-y_0)$$

的等式,由是,對於某一 c', 卽得

$$\left(D_{r-1}\binom{r}{r-1} ma_r (y-y_0)\right) \leqslant c' P^{-r+1-\rho t}.$$

故得(第一章引理 8, c) $G \ll G_0$, 於此,對應於定理中第 1, 2 及 3 三種情形,分別有

$$1)\quad G_0 = \frac{P}{q} m;\quad 2)\quad G_0 = m;\quad 3)\quad G_0 = m\frac{q}{P^{r-1}},$$

由是卽得 $G \ll mP^{1-\tau}$.

據此,由(5)卽可得出

$$|S|^{2b(k+h)} \ll P^{\frac{n(n+1)}{2}-\tau+(n+1)\rho t} m \int_0^1 \cdots \int_0^1 |T_1|^{2b(k+h)} d\alpha_1 \cdots d\alpha_n + Y^{2b(k+h)}.$$

令 $p_1 = P$, 我們現利用引理來估計 $|T_1|^{2b(k+h)}$. 我們有

$$|T_1|^{2b(k+h)} \ll \sum_{s_1=1}^{\eta_1} \cdots \sum_{s_k=1}^{\eta_k} \sum^{B} K(s_1, \cdots, s_k);$$

$$K(s_1, \cdots, s_k) = \sum_{(x_1, \cdots, x_{n+1})} e^{2\pi i (X_1 x_1 + \cdots + X_{n+1} x_{n+1})},$$

$$X_1 = \alpha_1 + \binom{2}{1}\alpha_2 x_0 + \cdots + \binom{n}{1}\alpha_n x_0^{n-1} + \binom{n+1}{1} m\alpha_{n+1} x_0^n,$$

$$X_2 = \alpha_2 + \cdots + \binom{n}{2}\alpha_n x_0^{n-2} + \binom{n+1}{2} m\alpha_{n+1} x_0^{n-1},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$X_n = \alpha_n + \binom{n+1}{n} m\alpha_{n+1} x_0,$$

$$X_{n+1} = m\alpha_{n+1}.$$

因之, $X_1 x_1 + \cdots + X_{n+1} x_{n+1} = A_1 \alpha_1 + \cdots + A_n \alpha_n + A_{n+1} m\alpha_{n+1}$,

於此

$$A_1 = x_1,$$

$$A_2 = \binom{2}{1} x_0 x_1 + x_2,$$

$$\cdots\cdots\cdots\cdots$$

$$A_n = \binom{n}{1} x_0^{n-1} x_1 + \binom{n}{2} x_0^{n-2} x_2 + \cdots + x_n,$$

$$A_{n+1}=\binom{n+1}{1}x_0^n x_1+\binom{n+1}{2}x_0^{n-1}x_2+\cdots+\binom{n+1}{n}x_0 x_n+x_{n+1}.$$

再,我們有

$$\int_0^1\cdots\int_0^1 K(s_1,\cdots,s_k)\,d\alpha_1\cdots d\alpha_n=$$

$$=\sum_{(x_1,\cdots,x_{n+1})}\int_0^1\cdots\int_0^1 e^{2\pi i\left(A_1\alpha_1+\cdots+A_n\alpha_n+A_{n+1}m\alpha_{n+1}\right)}\,d\alpha_1\cdots d\alpha_n,$$

而此(第一章引理 4)在數值上不大於數組 $(x_1,\cdots,x_{n+1})$ 中,其滿足條件 $A_1=\cdots=$ $=A_n=0$ 者的組數,不難看出,此種數組的數目卽等於數組 $(x_1,\cdots,x_{n+1})$ 中,其滿足條件 $x_1=\cdots=x_n=0$ 者的組數;而後面一數 $\ll\psi$, 因之,

$$|S|^{2b(k+h)}\ll P^{\frac{n(n+1)}{2}-\tau+(n+1)\rho t}m\sum_{s_1=1}^{\eta_1}\cdots\sum_{s_k=1}^{\eta_k}B\psi+Y^{2b(k+h)}\ll$$

$$\ll P^{\frac{n(n+1)}{2}-\tau+(n+1)\rho t}mP^{2b(k+h)-\frac{n(n+1)}{2}+\frac{n(n+1)}{2}\sigma}+Y^{2b(k+h)}\ll$$

$$\ll P^{2b(k+h)-\frac{5}{6}\tau\left(1-\frac{v}{15}\right)}m+Y^{2b(k+h)}.$$

定理的正確性現可由下之不等式得出:

$$\frac{\frac{5}{6}\tau\left(1-\frac{v}{15}\right)}{2b(k+h)}\geqslant\frac{\frac{5}{6}\tau\left(1-\frac{v}{15}\right)}{\frac{5}{2}\left(n+\frac{2}{5}\right)\left(\left(n-\frac{1}{2}\right)\ln\frac{3n(n+1)}{\tau}+n+3\right)}\geqslant$$

$$\geqslant\frac{\tau\left(1+\frac{v}{30}\right)}{3n^2\left(\ln\frac{3n(n+1)}{\tau}+\frac{(n+3)}{n-0.5}\right)}\geqslant\rho t,$$

$$\frac{1}{2b(k+h)}\geqslant\frac{2}{5\left(n-\frac{1}{5}\right)(n-1)\left(\ln\frac{12n(n+1)}{\tau}-1.4\right)}<\frac{2\rho}{\tau}.$$

例. 設多項式

$$F(x)=a_{n+1}x^{n+1}+\cdots+a_2x^2+a_1x$$

之係數 $a_{n+1},\cdots,a_2$ 中有一等於 $\sqrt{2}$, 而此多項式其餘各係數爲任意實數.

將 $\sqrt{2}$ 展成連分數,我們現來討論它的相隣諸漸近分數中,其分母 q 與 q' 滿足條件 $q\leqslant P<q'$ 者的一對. 由於部分商爲有界,故有 $q'\ll q$. 因之,所論的係數可以表成

$$\frac{a}{q}+\frac{\theta}{q^2}$$

的形式,於此 $(a, q)=1$, 且對某一 $c_1<1$,

$$c_1 P<q \leqslant P .$$

故由定理,即得

$$\sum_{x=1}^{P} e^{2\pi i m F(x)} \ll P^{1-\rho t} m^{2\rho};\quad \rho=\frac{1}{3n^2 \ln 12n(n+1)},\quad t=1+\frac{\nu}{30}.$$

定理 2, a. 設 P 與 N 爲整數, $P>0$, 又設在區間 $N \leqslant x \leqslant N+P$ 中,實函數 $f(x)$ 具有連續導數 $f^{(n+1)}(x)$, 滿足條件

$$\frac{1}{A_0} \leqslant\left|\frac{f^{n+1}(x)}{(n+1)!}\right| \leqslant \frac{c'}{A_0},$$

於此, $P \ll A_0 \ll P^{2+2\nu}$. 再設

$$S=\sum_{x=N+1}^{N+P} e^{2\pi i f(x)} .$$

則有

$$S \ll P^{1-\rho};\quad \rho=\frac{1}{3n^2 \ln 125\, n}.$$

證. 設

$$\nu_1=\frac{1}{n+1};\quad p_1=[A_0^{(1-\rho)\nu_1}];\quad k=\left[\frac{\ln(6n+6)}{-\ln(1-\nu)}+1\right].$$

則易得

$$k<\left(n-\frac{1}{2}\right) \ln(6n+6)+1;\quad \sigma<\frac{1}{6n+6}.$$

對 $y=N, \cdots, N+P-p_1$, 令

$$T_0=\sum_{x=1}^{p_1} e^{2\pi i(f(y+x)-f(y))},$$

則得(參看定理 1 的證明)

$$|S|=p_1^{-1} \sum_{y=N}^{N+P-p_1} T_0+\theta p_1;$$

$$|S|^{2b(k+h)} \ll p_1^{-2b(k+h)} P^{2b(k+h)-1} \sum_{y=N}^{N+P-p_1}|T_0|^{2b(k+h)}+p_1^{2b(k+h)}.$$

運用戴勞公式,即得

$$f(y+x)-f(y)=Y_1 x+\cdots+Y_n x^n+\theta \frac{c'}{A_0} p_1^{n+1},$$

$$Y_j = Y_j(y) = \frac{f^{(j)}(y)}{j!}; \quad \frac{c'}{A_0} p_1^{n+1} \ll P^{-\rho}.$$

置

$$T_1 = \sum_{x=1}^{p_1} e^{2\pi i\left(\alpha_1 x + \cdots + \alpha_n x^n\right)}.$$

若點 $(\alpha_1, \cdots, \alpha_n)$ 屬於 n 次元空間中由不等式

$$Y_1 - \frac{1}{2} p_1^{-1} P^{-\rho} \leqslant \alpha_1 \leqslant Y_1 + \frac{1}{2} p_1^{-1} P^{-\rho},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$Y_n - \frac{1}{2} p_1^{-n} P^{-\rho} \leqslant \alpha_n \leqslant Y_n + \frac{1}{2} p_1^{-n} P^{-\rho}$$

所定義的域 (Ω_y),則有

$$T_0 = T_1 + O(p_1 P^{-\rho}); \quad |T_0|^{2b(k+h)} \ll |T_1|^{2b(k+h)} + (p_1 P^{-\rho})^{2b(k+h)}.$$

將上之不等式兩邊乘以

$$p_1^{\frac{n(n+1)}{2}} P^{n\rho} d\alpha_1 \cdots d\alpha_n,$$

並就域 (Ω_y) 積分,則得

$$|T_0|^{2b(k+h)} \ll p_1^{\frac{n(n+1)}{2}} P^{n\rho} \int \underset{(\Omega y)}{\cdots} \int |T_1|^{2b(k+h)} d\alpha_1 \cdots d\alpha_n + (p_1 P^{-\rho})^{2b(k+h)}.$$

我們現來估計那種域 (Ω_y) 的數目 G, 它包含有一點,其位標與某一既定點 $(\alpha_1, \cdots, \alpha_n)$ 之位標僅在整數部份不同者. 設 (Ω_y) 與 (Ω_{y_0}) 爲這樣的兩個域;則

$$(Y_n(y) - Y_n(y_0)) \ll p_1^{-n} P^{-\rho} \ll P^{2\nu+\rho} A_0^{-1}.$$

因之(第一章引理 9, β, 置 $\Phi(y) = Y_n(y) - Y_n(y_0)$, $A = A_0(n+1)^{-1}$), $G \ll P^{2\nu+\rho}$. 由是我們有

$$S^{2b(k+h)} \ll p_1^{-2b(k+h) + \frac{n(n+1)}{2}} P^{2h(k+h) - 1 + 2\nu + (n+1)\rho} \times$$

$$\times \int_0^1 \cdots \int_0^1 |T_1|^{2b(k+h)} d\alpha_1 \cdots d\alpha_n + F,$$

$$F = p_1^{2b(k+h)} + p_1^{-2b(k+h)} P^{2b(k+h)} (p_1 P^{-\rho})^{2b(k+h)} \ll (P^{1-\rho})^{2b(k+h)}.$$

我們現運用引理來估計 $|T_1|^{2b(k+h)}$. 如是卽得

$$|T_1|^{2b(k+h)} \ll \sum_{S_1=1}^{\eta_1} \cdots \sum_{S_k=1}^{\eta_k} \sum^{B} K(s_1, \cdots, s_k),$$

$$K(s_1, \cdots, s_k) = \sum_{(x_1, \cdots, x_{n+1})} e^{2\pi i\left(X_1 x_1 + \cdots + X_n x_n\right)},$$

$$X_1 = \alpha_1 + \binom{2}{1} \alpha_2 x_0 + \cdots + \binom{n}{1} \alpha_n x_0^{n-1},$$

$$X_2 = \qquad \alpha_2 \quad + \cdots + \binom{n}{2} \alpha_n x_0^{n-2},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

$$X_n = \qquad\qquad \alpha_n.$$

再,我們有

$$X_1 x_1 + \cdots + X_n x_n = A_1 \alpha_1 + \cdots + A_n \alpha_n,$$

$$A_1 = x_1,$$

$$A_2 = \binom{2}{1} x_0 x_1 + x_2,$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$A_n = \binom{n}{1} x_0^{n-1} x_1 + \binom{n}{2} x_0^{n-2} x_2 + \cdots + x_n.$$

依據第一章引理 4, 積分

$$\int_0^1 \cdots \int_0^1 K(s_1, \cdots, s_k)\, d\alpha_1 \cdots d\alpha_k = \sum_{(x_1, \cdots, x_{n+1})} \int_0^1 \cdots \int_0^1 e^{2\pi i\left(A_1\alpha_1 + \cdots + A_n\alpha_n\right)}\, d\alpha_1 \cdots d\alpha_n$$

等於數組 $(A_1, \cdots, A_n)$ 中其滿足條件 $A_1 = \cdots = A_n = 0$ 者的組數. 但這數目顯然等於數組 $(x_1, \cdots, x_{n+1})$ 中其滿足條件 $x_1 = \cdots = x_n = 0$ 者的組數; 即 $\ll \psi$. 因之

$$\int_0^1 \cdots \int_0^1 |T_1|^{2b(k+h)}\, d\alpha_1 \cdots d\alpha_n \ll$$

$$\ll \sum_{S_1=1}^{\eta_1} \cdots \sum_{S_k=1}^{\eta_k} B\psi \ll p_1^{2b(k+h) - \frac{n(n+1)}{2} + \frac{n(n+1)}{2}\sigma},$$

$$S^{2b(k+h)} \ll P^{2b(k+h) - 1 + 2\nu + (n+1)\rho}\, p_1^{\frac{n(n+1)}{2}\sigma} + P^{(1-\rho)2b(k+h)} \ll$$

$$\ll P^{2b(k+h) - \frac{5}{6} + \frac{25}{12}\nu} + P^{(1-\rho)2b(k+h)}.$$

定理之正確性現由下之不等式卽可推出

$$\frac{\frac{5}{6}-\frac{25}{12}\nu}{2b(k+h)} \geqslant \frac{\frac{5}{6}(1-2.5\nu)}{\frac{5}{2}\left(n+\frac{2}{5}\right)\left(n-\frac{1}{2}\right)\left(\ln(6n+6)+\frac{4}{3}\right)} \geqslant$$

$$\geqslant \frac{1}{3n^2(1+3.1\nu)(\ln n+3.2)} > \rho .$$

定理 2, b. 設 N 與 P 爲整數, $P>0$; 在區間 $N \leqslant x \leqslant N+P$ 中,實函數 $f(x)$ 具有連續導數 $f^{(n+1)}(x)$, 滿足條件

$$\frac{1}{A_0} \leqslant \left|\frac{f^{(n+1)}(x)}{(n+1)!}\right| \leqslant \frac{c'}{A_0},$$

於此, $P \ll A_0 \ll P^{2+\nu}$. 又設在同一區間中, $\Phi(x)$ 爲單調,且 $\max|\Phi(x)| \ll \Phi_0$.

若用字母 P_1 記區間 $1 \leqslant P_1 \leqslant P$ 中之任一整數,並令

$$S(P_1)=\sum_{x=N+1}^{N+P_1} \Phi(x)\, e^{2\pi i f(x)},$$

則有

$$S(P_1) \ll \Phi_0 P^{1-\rho}; \quad \rho=\frac{1}{3n^2 \ln 125\, n}.$$

證. 對於屬於區間 $1 \leqslant P_0 \leqslant P$ 中之整數 P_0, 我們引入記號

$$\sigma(P_0)=\sum_{x=N+1}^{N+P_0} e^{2\pi i f(x)}.$$

當 $A_0^{(2+2\nu)^{-1}} \leqslant P_0 \leqslant P$, 依據定理 2, a, 我們有

$$\sigma(P_0) \ll P_0^{1-\rho} \ll P^{1-\rho}. \tag{6}$$

當 $1 \leqslant P_0 \leqslant A_0^{(2+2\nu)^{-1}}$, 不等式 (6) 可由

$$\sigma(P_0) \ll P_0 \ll P^{(2+\nu)(2+2\nu)^{-1}} \ll P^{1-\rho}$$

得出. 因之,不等式 (6) 對 $1 \leqslant P_0 \leqslant P$ 皆成立. 運用亞培爾 (Abel) 變換於和數 $S(P_1)$, 我們即已證明定理.

例. 設 $s=\sigma+it$, $\sigma>0$, $t>1$, P 及 P_1 爲整數,

$$t^{\frac{1}{n}} \leqslant P \leqslant t^{\frac{1}{n-1}}; \quad 1 \leqslant P_1 \leqslant P.$$

我們現運用定理 2, b 來估計和數

$$S=\sum_{x=P+1}^{P+P_1}\frac{1}{x^s}.$$

於此,我們有

$$S=\sum_{x=P+1}^{P+P_1}\Phi(x)\,e^{2\pi if(x)};\quad \Phi(x)=\frac{1}{x^\sigma};\quad f(x)=\frac{-t\ln x}{2\pi},$$

$$\left|\frac{f^{(n+1)}(x)}{(n+1)!}\right|=\frac{t}{2\pi(n+1)x^{n+1}}.$$

令

$$A_0=\frac{2\pi(n+1)2^{n+1}P^{n+1}}{t};\quad c'=2^{n+1},$$

則有

$$P\ll A_0\ll P^2;\quad \frac{1}{A_0}\leqslant\left|\frac{f^{(n+1)}(x)}{(n+1)!}\right|\leqslant\frac{c'}{A_0};\quad \max\frac{1}{x^\sigma}=\frac{1}{P^\sigma}.$$

因之,

$$S\ll\frac{1}{P^\sigma}P^{1-\rho}=P^{1-\sigma-\rho};\quad \rho=\frac{1}{3n^2\ln 125\,n}.$$

第 七 章

華林問題中的漸近公式

在本章裏,我要來證明,對於將正整數 N 表成

$$N=x_1^n+\cdots+x_r^n;\quad x_1>0,\cdots,x_r>0$$

的表法的種數,哈代與李托伍德所得到的漸近公式當

$$r\geqslant[10\,n^2\ln n]$$

時不爲膚淺.

爲了證明此說,我現來研究一個積分,它與哈代和李托伍德在解決華林問題時所使用的積分相似,但我現在用以我自己的方法所得到的估值去代替以外爾氏方法所得到的估值.

專用記號. 在本章中,我們將假定 $n\geqslant 12$, 並採用下列記號:

$$b=\left[\frac{5}{4}n+\frac{1}{2}\right];\ h=n+2;\ k=\left[\frac{\ln(0.6\,n^2\ln 12\,n^2)}{-\ln(1-\nu)}+1\right];\ \sigma=(1-\nu)^k.$$

引理. 設 p_1 爲整數，$p_1>1$；$a_n, \cdots, a_1$ 爲固定整數；

$$f(x)=a_n x^n+\cdots+a_1 x,\ a_n>0;$$

$$T_1=\sum_{x=1}^{p_1} e^{2\pi i \alpha f(x)}.$$

則有

$$\int_0^1 |T_1|^{2b(k+h)}\,d\alpha \ll p_1^{2b(k+h)-n+\frac{n(n+1)}{2}\sigma}.$$

證. 運用第六章之引理,我們有

$$T_1^{2b(k+h)} \ll \sum_{s_1=2}^{\eta_1}\cdots\sum_{s_k=2}^{\eta_k}\sum^{B} K(s_1,\cdots,s_k),$$

$$K(s_1,\cdots,s_k)=\sum_{x_1=-[cp_1]}^{[cp_1]}\cdots\sum_{x_n=-[cp_1^n]}^{[cp_1^n]} \psi(x_1,\cdots,x_n)\, e^{2\pi i\alpha(X_1x_1+\cdots+X_nx_n)},$$

$$X_j=\frac{f^{(j)}(x_0)}{j!};\ X_n=a_n,$$

此處的 x_0 是整數；

$$\psi(x_1,\cdots,x_n)\ll\psi;\ B\psi\ll p_1^{2b(k+h)-\frac{n(n+1)}{2}+\frac{n(n+1)}{2}\sigma}\,2^{-4(s_1+\cdots+s_k)}.$$

但積分

$$\int_0^1 e^{2\pi i\alpha(X_1x_1+\cdots+X_nx_n)}\,d\alpha$$

當

$$X_1x_1+\cdots+X_nx_n=0 \tag{1}$$

時爲 1，在另外的情形爲 0. 又因對於每一組所給的值 $x_1, \cdots, x_{n-1}$，最多只有一個值 x_n 滿足不定方程 (1)，因而滿足此不定方程之數組 $(x_1, \cdots, x_n)$，總數將

$$\ll p_1\cdots p_1^{n-1}=p_1^{\frac{n(n-1)}{2}}.$$

故得

$$\int_0^1 K(s_1,\cdots,s_k)\,d\alpha\ll p_1^{\frac{n(n-1)}{2}}\psi;$$

$$\int_0^1 T_1^{2b(k+h)}\,d\alpha\ll\sum_{s_1=1}^{\eta_1}\sum_{s_k=1}^{\eta_k} p_1^{\frac{n(n-1)}{2}}B\psi\ll$$

$$\ll\sum_{s_1=1}^{\eta_1}\cdots\sum_{s_k=1}^{\eta_k} p_1^{2b(k+h)-n+\frac{n(n+1)}{2}\sigma}\,2^{-4(s_1+\cdots+s_k)}\ll$$

$$\ll p_1^{2b(k+h)-n+\frac{n(n+1)}{2}\sigma}.$$

定理. 對於以正整數 $x_1, \cdots, x_n$ 將正整數 N 表成

$$N = x_1^n + \cdots + x_r^n$$

的表法的種數,哈代與李托伍德所得到的公式

$$I(N) = \frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu)} N^{\nu r-1} \mathfrak{S} + O(N^{r\nu-1-\nu^2}); \mathfrak{S} = \sum_{q=1}^{\infty} A(q)$$

(用第二章之記號)當

$$r \geqslant [10 n^2 \ln n]$$

時成立.

證. 令

$$p_1 = [N^\nu], \tau = 2n p_1^{n-1}; T_1 = \sum_{x=1}^{p_1} e^{2\pi i \alpha x^n},$$

則得

$$I(N) = \int_{-\tau^{-1}}^{1-\tau^{-1}} T_1^r e^{-2\pi i \alpha N} d\alpha.$$

我們將積分區間分成基本區間,即包含所有滿足條件

$$\alpha = \frac{a}{q} + z; \quad (a, q) = 1; \frac{-1}{q\tau} \leqslant z \leqslant \frac{1}{q\tau}; 0 < q \leqslant p_1^{1-\nu}$$

之 α 的區間,和餘區間,即包含所有遺留下來的 α 的區間. 對於餘區間,我們有

$$\alpha = \frac{a}{q} + z, (a, q) = 1; |z| \leqslant \frac{1}{q\tau}; p_1^{1-\nu} < q \leqslant \tau.$$

設 $I_0(N)$ 爲積分 $I(N)$ 對應於基本區間之部分, $I_1(N)$ 爲對應於餘區間之部分. 則

$$I(N) = I_0(N) + I_1(N).$$

由於 $[10n^2 \ln n] > 2n + 1$, 故對 $I_0(N)$ 可以運用第三章中最後的公式;我們卽得

$$I_0(N) = \frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu)} N^{r\nu-1} \sum_{0<q\leqslant p_1^{1-\nu}} A(q) + O(N^{r\nu-1-\nu^2}).$$

由第二章引理 6, 我們有

$$\sum_{q>p_1^{1-\nu}} A(q) \ll \sum_{q>p_1^{1-\nu}} q^{1-(2n+2)\nu} \ll p_1^{-(1-\nu)2\nu} \ll N^{-\nu^2}.$$

因之,

$$I_0(N)=\frac{(\Gamma(1+\nu))^r}{\Gamma(r\nu)}N^{r\nu-1}\mathfrak{S}+O(N^{r\nu-1-\nu^2}).$$

我們現來估計 $I_1(N)$. 由引理,我們有

$$\int_0^1 |T_1|^{2b(k+h)}\,d\alpha \ll p_1^{2b(k+h)-n+\frac{n(n+1)}{2}\sigma}.$$

再,由第六章定理 1,我們有

$$T_1 \ll p_1^{1-\rho_1};$$

$$\rho_1=\frac{1-\nu}{3(n-1)^2\ln\frac{12n(n-1)}{1-\nu}}=\frac{1}{3n(n-1)\ln 12n^2}.$$

故得

$$I_1(N)\ll p_1^{(r-2b(k+h))\left(1-\frac{1}{3n(n-1)\ln 12n^2}\right)+2b(k+h)-n+\frac{n(n+1)}{2}\sigma}\ll$$

$$\ll p_1^{r-n+\frac{n(n+1)}{2}\sigma-\frac{r-2b(k+h)}{3n(n-1)\ln 12n^2}}=p_1^{r-n-\delta},$$

於此,我們有

$$\delta>-\frac{n(n+1)}{1.2n^2\ln 12n^2}+$$

$$+\frac{10n^2\ln n-1-(2.5n+1)((n-0.5)\ln(0.6n^2\ln 12n^2)+n+3)}{3n(n-1)\ln 12n^2}>$$

$$>\frac{-5n(n-\nu)+20n^2\ln n-2-(5n+2)((n-0.5)\,2.8\ln n+n+3)}{6n(n-1)\ln 12n^2}>\frac{1}{12}.$$

由是即得我們的定理.

第　八　章

整多項式值的分數部份的分佈

在本章裏,我們要運用普遍方法來導出一個漸近公式,這公式是表出數列

$$\{F(x)\};\ x=1,\cdots,P$$

中,其小於一既定眞分數之分數的個數者.

在這裏,我們只限於討論 $F(x)$ 爲一實係數整多項式的情形. 多項式的次數,

如前一章一樣,看作是固定的；但同樣的方法也適用於次數慢慢增長的情形(隨函數 $F(x)$ 的形狀及區間長 P 之改變而增長).

定理. 設 P 爲一正整數，$n \geqslant 11$；$F(x) = a_{n+1}x^{n+1} + \cdots + a_1 x$；$a_{n+1}, \cdots, a_1$ 爲實數；s 爲 $n+1, \cdots, 2$ 中之一；

$$a_s = \frac{a}{q} + \frac{\theta}{q^2};\ (a, q) = 1,\ q > 0.$$

則對任何滿足條件 $0 < \gamma < 1$ 之 γ，數列

$$\{F(x)\};\ x = 1, \cdots, P$$

中,其滿足條件 $0 \leqslant \{F(x)\} < \gamma$ 之分數的個數 T 可以表成公式

$$T = \gamma P + O(P^{1-\rho});\ \rho = \frac{\tau}{3n^2 \ln \dfrac{12n(n+1)}{\tau}},$$

這裏的 τ 由下之等式所定義:

$$\begin{aligned} q &= c_1 P^{\tau}, && 若\ 1 < q \leqslant c_1 P; \\ \tau &= 1, && 若\ c_1 P \leqslant q \leqslant c_2 P^{s-1}; \\ q &= c_2 P^{s-\tau}, && 若\ c_2 P^{s-1} \leqslant q < c_3 P^{s}, \end{aligned}$$

且服從條件 $\tau \geqslant \tau_0$，此處 τ_0 爲一正常數(任意小).

證. 設

$$\Delta_0 = P^{-\rho h};\ \Delta = P^{-\rho};\ h = 1 + \frac{\nu}{30};\ S_m = \sum_{x=1}^{P} e^{2\pi i m F(x)}.$$

則由第六章定理 1，有

$$S_m \ll m^{2\rho\tau^{-1}} P \Delta_0.$$

若 $\Delta \geqslant 0.25$，則定理顯然成立；故我們只討論 $\Delta < 0.25$ 之情形. 任取滿足條件 $0 \leqslant B - A \leqslant 1 - 2\Delta$ 之實數 A 及 B，我們現來討論第一章引理 12 中所述的以 1 爲週期之函數 $\psi(x)$，但此時假定

$$r = 1,\ \alpha + \frac{1}{2}\Delta = A,\ \beta - \frac{1}{2}\Delta = B.$$

由是卽有

$$\psi(F(x)) = 1,\ 若\ A \leqslant F(x) \leqslant B \pmod 1;$$
$$0 \leqslant \psi(F(x)) \leqslant 1,\ 若\ A - \Delta \leqslant F(x) \leqslant A \pmod 1,$$
$$或\ B \leqslant F(x) \leqslant B + \Delta \pmod 1;$$

$$\psi(F(x))=0, \text{ 若 } B+\Delta\leqslant F(x)\leqslant A-\Delta+1 \pmod 1;$$

$$\psi(F(x))=(B-A+\Delta)+\sum_{m=1}^{\infty}(a_m\cos 2\pi mF(x)+b_m\sin 2\pi mF(x)), \tag{1}$$

於此，

$$a_m\ll\frac{1}{m},\ b_m\ll\frac{1}{m}, \text{ 若 } m\leqslant\frac{1}{\Delta};$$

$$a_m\ll\frac{1}{\Delta m^2},\ b_m\ll\frac{1}{\Delta m^2}, \text{ 若 } m>\frac{1}{\Delta}.$$

由 (1) 即得

$$\sum_{x=1}^{P}\psi(F(x))=P(B-A+\Delta)+\sum_{m=1}^{\infty}(a_m S'_m+b_m S''_m),$$

此處的 S'_m 及 S''_m 係由等式 $S_m=S'_m+iS''_m$ 所定義. 因之

$$\sum_{m=1}^{\infty}(a_m S'_m+b_m S''_m)\ll\sum_{0<m\leqslant\Delta^{-1}}\frac{m^{2\rho\tau-1}P\Delta_0}{m}+\sum_{\Delta^{-1}<m\leqslant\Delta^{-2}}\frac{m^{2\rho\tau-1}P\Delta_0}{\Delta m^2}+$$

$$+\sum_{m>\Delta^{-2}}\frac{P}{\Delta m^2}\ll\Delta^{-2\rho\tau-1}P\Delta_0+P\Delta\ll P^{2\rho^2\tau^{-1}+1-\frac{\rho\nu}{30}}\Delta+P\Delta\ll P\Delta,$$

$$\sum_{x=1}^{P}\psi(F(x))=P(B-A)+O(P\Delta). \tag{2}$$

用記號 $T(A;B)$ 記 $F(x)$ 的諸值中，其滿足條件 $A\leqslant F(x)<B \pmod 1$ 者的個數. 則等式 (2) 可以化成

$$\theta_1 T(A-\Delta;A)+T(A;B)+\theta_2 T(B;B+\Delta)=P(B-A)+O(P\Delta),$$

$$\theta_1\geqslant 0;\ \theta_2\geqslant 0;$$

因之，由顯然的不等式 $T(A-\Delta;A)\ll P\Delta$, $T(B;B+\Delta)\ll P\Delta$, 此可由 (2) 先以 $A-\Delta$ 及 A 代 A 及 B, 再以 B 及 $B+\Delta$ 代 A 及 B 而得，我們卽有

$$T(A;B)=P(B-A)+O(P\Delta).$$

由是卽得

$$T=T\left(0;\frac{1}{2}\gamma\right)+T\left(\frac{1}{2}\gamma;\ \gamma\right)=P\left(\frac{1}{2}\gamma-0\right)+P\left(\gamma-\frac{1}{2}\gamma\right)+$$

$$+O(P\Delta)=P\gamma+O(P\Delta),$$

此卽證明我們的定理.

第 九 章

以素數爲求和變數的最簡單三角和數的估値

在本章裏，我將運用我的方法來推出形如

$$\sum_{p\leqslant N} e^{2\pi i\alpha p}$$

的和數的估値，這裏的 α 是實數，p 跑過素數．這項估値是取決於數 α 的有理近逼．

在這裏，我不作更一般形式的和數的估値．然而必須注意，同樣的方法也有可能用來估計形如

$$\sum_{p\leqslant N} e^{2\pi i f(p)}$$

的和數，這裏的 $f(p)$ 可以是高於一次的整多項式（此時所得的估値是決定於 p 的高於一次方的係數的有理近逼），也可以是依某種意義而言可以用整多項式去密切逼近的函數．

同樣的方法也有可能用來估計以素數爲求和變數的純算術和．例如形如

$$\sum_{p\leqslant N} \chi(p+k)$$

的和數很簡單的就可估計出來，這裏的 $\chi(a)$ 是一關於模 q 的非主特徵，$(k, q)=1$．而在一般的情形，將我的方法與英國數學家的方法結合起來，則可以估計形如

$$\sum_{p\leqslant N} \chi(f(p))$$

的和數，這裏的 $f(p)$ 是一整值整多項式．

最後，必須要指出，在所有列舉的問題中，其跑過素數的變數 p 可代以跑過別的數列的變數，如屬於一算術級數中的素數所成之數列，使 $\mu(a)\chi(a)$ 具有旣定數值的整數 a 所成之數列，由非常一般形狀的乘積所組成的數列等等．

專用記號． 在本章裏，p 常表示素數，N 爲 $\geqslant C_0$ 的整數，C_0 是一充分大的數；此外，我們並假定 $r=\ln N$．

引理 1． 設 u 跑過由兩個因子作成的積，這兩個因子互相獨立地各跑過一個由正整數作成的增加數列，又設 v 跑過一個由正整數作成的增加數列，$1<U<N$，$U<U'\ll U$；

$$\alpha=\frac{a}{q}+\frac{\theta}{q^2};\qquad (a,q)=1;\qquad 1<q<N,$$

$$S=\sum_{U<u\leqslant U'}\sum_{v\leqslant Nu^{-1}} e^{2\pi i\alpha uv}.$$

則有

$$S\ll Nr^2\sqrt{\frac{1}{q}+\frac{q}{N}+\frac{1}{U}+\frac{U}{N}}.$$

證．當 u 跑過上述數值時，不定方程式 $u=z$ 的解數 $\leqslant\tau_2(z)$，而（第一章引理 17, b）

$$\sum_{z\leqslant U'}(\tau_2(z))^2\ll Ur^3.$$

因之，若令 z 連區間 $U<z\leqslant U'$ 內之所有整數一起跑過，則有

$$S^2\ll Ur^3\sum_{U<z\leqslant U'}\left|\sum_{v\leqslant Nz^{-1}} e^{2\pi i\alpha zv}\right|^2=$$

$$=Ur^3\sum_{U<z\leqslant U'}\sum_{v'\leqslant Nz^{-1}}\sum_{v\leqslant Nz^{-1}} e^{2\pi i\alpha z(v'-v)}.$$

我們再將求和記號改變次序．顯而易見，v' 與 v 只能跑過不大於 NU^{-1} 的那種數值；而當 v' 與 v 給定時，z 則跑過區間

$$U<z\leqslant\min\left(U',\frac{N}{v'},\frac{N}{v}\right).$$

中的整數．故得（第一章引理 6），

$$S^2\ll Ur^3\sum_{v'\leqslant NU^{-1}}\sum_{v\leqslant NU^{-1}}\min\left(U,\frac{1}{2(\alpha(v'-v))}\right),$$

由是，若注意長爲 $\ll NU^{-1}$ 之區間可以分成 $\ll NU^{-1}q^{-1}+1$ 個其長 $\leqslant q$ 之區間，則我們卽得（第一章引理 8, a）

$$S^2\ll Ur^3\frac{N}{U}\left(\frac{N}{Uq}+1\right)(U+q\log q)\ll N^2r^4\left(\frac{1}{q}+\frac{q}{N}+\frac{1}{U}+\frac{U}{N}\right).$$

引理 2. 設 P 爲正整數；z 跑過整數 $z_1,\cdots,z_n$；S' 記當 z 跑過與 P 互素之 z 值時，函數 $f(z)$ 所取之值之和；S_d 記當 z 跑過其爲 d 之倍數之 z 值時，函數 $f(z)$ 所取之值之和．則

a)
$$S'=\sum_{d/P}\mu(d)S_d.$$

b）若對所說的 z 值有 $f(z)\geqslant 0$，且 m 爲一偶正整數，則

$$S' \leqslant \sum_{\substack{d/P \\ \Omega(d) \leqslant m}} \mu(d) S_d.$$

定理 1. 設 $H = e^{\frac{1}{2}\sqrt{r}}$,

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2}; \quad (a, q) = 1; \quad 1 < q < N; \quad S = \sum_{p \leqslant N} e^{2\pi i \alpha p}.$$

則有

$$S \ll N r^{4,5} \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H} \right).$$

證. 設P爲不超過 $\sqrt{N}$ 的所有素數的乘積. 令 z 跑過區間 $0 < z \leqslant N$ 中之整數. 設

$$f(z) = e^{2\pi i \alpha z},$$

並運用引理 2, a. 我們卽得

$$S' = \sum_{d/P} \mu(d) S_d; \qquad S' = e^{2\pi i \alpha} + \sum_{\sqrt{N} < p \leqslant N} e^{2\pi i \alpha p} =$$

$$= S + O(\sqrt{N}); \qquad S_d = \sum_{0 < m \leqslant N d^{-1}} e^{2\pi i \alpha d m}.$$

由是卽得

$$S = S_0 - S_1 + O(\sqrt{N}); \qquad S_0 = \sum\sum_{d_0 m \leqslant N} e^{2\pi i \alpha d_0 m}; \ S_1 = \sum\sum_{d_1 m \leqslant N} e^{2\pi i \alpha d_1 m},$$

於此, d_0 跑過 P 的因子中滿足條件 $\mu(d) = 1$ 者; d_1 跑過 P 的因子中滿足條件 $\mu(d) = -1$ 者; 最後, m 則跑過正整數.

下面, 我們只限於估計和數 S_0, 因爲和數 S_1 可以同法估計. 我們將區間 $0 < m \leqslant N$ 分成 $\ll r$ 個形如

$$M < m \leqslant M'; \qquad M < M' \leqslant 2M \tag{1}$$

之區間. 和數 S_0 中對應於區間 (1) 之部分, 我們以 $S(M)$ 記之.

我們先來研究 $M \geqslant H$ 之情形; 此時, 若假定 $M(d_0) = \min\,(M', N d_0^{-1})$, 則有

$$S(M) = \sum_{d_0 < N M^{-1}} \sum_{M < m \leqslant M(d_0)} e^{2\pi i \alpha d_0 m} \ll \sum_{d_0 < M N^{-1}} \min\left(\frac{N}{d_0}, \frac{1}{2(\alpha d_0)} \right),$$

由是, 我們卽得 (第一章引理 8, b)

$$S(M) \ll \left(\frac{N}{M} + q + \frac{N}{q} \right) r \ll N r \left(\frac{1}{H} + \frac{q}{N} + \frac{1}{q} \right).$$

現在剩下來的只是去研究 $M<H$ 的情形．將和數 $S(M)$ 表成

$$S(M)=\sum_{M<m\leqslant M'}\sum_{d_0\leqslant Nm^{-1}}e^{2\pi iad_0m}$$

的形式．我們用記號 δ_k 來記每一個恰好具有 k 個大於 H^2 的素因子的 d_0．設 k_0 爲當 $d_0\leqslant N$ 時諸 k 值中最大的一個；由 $2^{k_0}\leqslant N$，卽得 $k_0\ll r$．我們有

$$S(M)=\sum_{0\leqslant k\leqslant k_0}S_k(M);\quad S_k(M)=\sum_{M<m\leqslant M'}\sum_{\delta_k\leqslant Nm^{-1}}e^{2\pi ia\delta_km}.$$

我們先來討論 $S_0(M)$．對於 $\delta_0>NM^{-1}H^{-1}$，令 $\Omega(\delta_0)=\kappa$，卽得

$$H^{2\kappa}>NH^{-2};\quad (2\kappa+2)\,0.5\sqrt{r}>r;\quad \kappa>\sqrt{r}-1;\quad \tau(\delta_0)>2^{\sqrt{r}-1}.$$

利用後一不等式及第一章引理 17,c，我們卽得

$$S_0(M)\ll\sum_{M<m\leqslant M'}\left(\sum_{\delta_0\leqslant NM^{-1}H^{-1}}1+\sum_{NM^{-1}H^{-1}<\delta_0\leqslant Nm^{-1}}\frac{\tau(\delta_0)}{2^{\sqrt{r}}}\right)\ll$$

$$\ll M\left(\frac{N}{HM}+\frac{Nr}{M2^{\sqrt{r}}}\right)\ll\frac{N}{H}.$$

我們再來討論當 $k>0$ 時之 $S_k(M)$．我們將和數 $S_k(M)$ 與和數

$$T_k=\sum_{M<m\leqslant M'}\sum_{pt\leqslant Nm^{-1}}\sum e^{2\pi iaptm}$$

比較，於此，p 跑過區間 $H^2<p\leqslant\sqrt{N}$ 中之素數，而 t 則跑過恰好具有 $k-1$ 個大於 H^2 的素因子的 d_1．

設 $k>1$．對和數 T_k 中，其 $(p,t)=p$ 之諸項，顯然有

$$\ll\sum_{M<m\leqslant M'}\sum_{H^2<p\leqslant\sqrt{N}}\frac{NM^{-1}}{p^2}\ll M\frac{NM^{-1}}{H^2}<\frac{N}{H}.$$

和數 T_k 中留下來的那些項也就是和數 $S_k(M)$ 中的那些項，但和數 $S_k(M)$ 中的每一項在和數 T_k 中恰好出現 k 次．因之，

$$S_k(M)=\frac{1}{k}T_k+O\left(\frac{N}{kH}\right).$$

上之不等式當 $k=1$ 時顯然也成立，但此時餘下的項則等於 0．

我們來估計 T_k．令 $mp=u$，我們將區間

$$MH^2<u\leqslant M'\sqrt{N}$$

分成 $\ll r$ 個形如

$$Q<u\leqslant Q';\quad Q<Q'\leqslant 2Q \tag{2}$$

之區間．令 $T_k(Q)$ 爲和數 T_k 中對應於區間（2）之部分；我們有

$$T_k(Q) = \sum_{Q<u\leqslant Q'} \sum_{ut\leqslant N} e^{2\pi i a u t};$$

由是，運用引理 1，我們即得

$$T_k(Q) \ll N r^2 \sqrt{\frac{1}{q} + \frac{q}{N} + \frac{1}{H^2} + \frac{M\sqrt{N}}{N}} \ll N r^2 \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right),$$

$$S_k(M) \ll \frac{1}{k} N r^3 \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right); \quad S(M) \ll N r^{3.5} \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right),$$

$$S_0 \ll N r^{4.5} \left(\sqrt{\frac{1}{q} + \frac{q}{N}} + \frac{1}{H}\right).$$

引理 3. 設 $x > 2$. 則

$$\sum_{p\leqslant x} \frac{1}{p} = c + \ln\ln x + O\left(\frac{1}{\ln x}\right); \quad \prod_{p\leqslant x}\left(1 - \frac{1}{p}\right) = \frac{c_0}{\ln x} + O\left(\frac{1}{(\ln x)^2}\right).$$

引理 4. 設

$$b = e^{r^{1-1.5\varepsilon}}; \; b_1 = e^{r^{1-2\varepsilon}}; \; 0 < q < b_1; \; 0 \leqslant l < q; \; (l, q) = 1; \; U \geqslant 0; \; W \geqslant b.$$

則對於形如 $qx + l$ 且不爲 $\leqslant b_1$ 的素數所除盡而又滿足條件

$$U < qx + l \leqslant U + W \tag{3}$$

的數的個數 T，有不等式

$$T \ll \frac{W (rq)^{2\varepsilon}}{rq}.$$

證．設 $p_1, \cdots, p_\sigma$ 皆爲素數，不超過 b_1，且除不盡 q，又設 P 爲它們的積，因而 $\Omega(P) = \sigma$．置 $m = 2\,[2\ln r + 1]$．令 z 跑過所有滿足條件（3）的整數 $qx + l$，又令 $f(z) = 1$，運用引理 2, b，我們即得

$$T \ll \sum_{\substack{d/P \\ \Omega(d)\leqslant m}} \mu(d)\, S_d,$$

於此，S_d 爲所有滿足條件（3）且爲 d 之倍數的 $qx + l$ 的個數．但

$$S_d = \frac{W}{qd} + \theta_d.$$

因之，

$$T \ll \left| \sum_{\substack{d/P \\ \Omega(d)\leqslant m}} \mu(d) \frac{W}{qd} \right| + \sum_{s=0}^{m} \binom{\sigma}{s}.$$

再,我們有 (引理 3 及第一章引理 17, a)

$$\sum_{d/P}\mu(d)\frac{W}{qd}=\frac{W}{q}\frac{\prod\limits_{p\leqslant b_1}\left(1-\frac{1}{p}\right)}{\prod\limits_{p/q}\left(1-\frac{1}{p}\right)}\ll\frac{Wq^{2\varepsilon}}{qr^{1-2\varepsilon}}=\frac{W(rq)^{2\varepsilon}}{rq};$$

$$\left|\sum_{\substack{d/P\\ m<\Omega(d)\leqslant\sigma}}\mu(d)\frac{W}{qd}\right|\ll\frac{W}{q}\sum_{s=m+1}^{\sigma}\sum_{\substack{d/P\\ \Omega(d)=s}}\frac{1}{d}<\frac{W}{q}\sum_{s=m+1}^{\sigma}\frac{\left(\frac{1}{p_1}+\cdots+\frac{1}{p_\sigma}\right)^s}{s!}<$$

$$<\frac{W}{q}\sum_{s=m+1}^{\sigma}\left(\frac{e(c_2+\ln r)}{s}\right)^s\ll\frac{W}{q}\sum_{s=m+1}^{\sigma}\left(\frac{3}{4}\right)^s\ll\frac{W}{rq}.$$

最後,

$$\sum_{s=0}^{m}\binom{\sigma}{s}<\sum_{s=0}^{m}\sigma^s\ll b_1^m<\frac{W}{rq}\frac{rq}{b}b_1^{5\ln r}\ll\frac{W}{rq}.$$

由是,我們的引理卽已證明.

定理 2, a. 設 $b_1=e^{r^{1-2\varepsilon}}$, $Nb_1^{-1}\leqslant A\leqslant N$,

$$(a,q)=1,\qquad 0<q\leqslant e^{r^{\varepsilon}},\qquad S=\sum_{N-A<p\leqslant N}e^{2\pi i\frac{a}{q}p}.$$

則有

$$S\ll\frac{A(rq)^{5\varepsilon}}{r\sqrt{q}}.$$

證. 設 $b_0=e^{r^{1-\varepsilon}}$, $b=e^{r^{1-1.5\varepsilon}}$, P 爲所有不超過 b_0 並除不盡 q 之素數之積. 令 z 跑過區間 $N-A<z\leqslant N$ 中與 q 互素的數,並設

$$f(z)=e^{2\pi i\frac{a}{q}z},$$

運用引理 2, a, 我們卽得

$$\sum_{\substack{N-A<z\leqslant N\\ (z,P)=1\\ (z,q)=1}}e^{2\pi i\frac{a}{q}z}=\sum_{d/P}\mu(d)S_d,\tag{4}$$

於此有

$$S_d=\sum_{\substack{\frac{N-A}{d}<m\leqslant\frac{N}{d}\\ (m,q)=1}}e^{2\pi i\frac{ad}{q}m}.$$

在討論 S_d 的同時,我們現跟着來討論 Z_d, 這裏的 Z_d 是表示形如 $qx+l$ 的整數中,其爲 d 之倍數且屬於區間 $N-A<qx+l\leqslant N$ 者的個數. 若 $d<N^{0.8}$,

則若將 S_d 中出現之每一 m 用其關於模 q 之最小非負剩餘來代替，我們即得

$$S_d = \frac{A}{qd} \sum_{\substack{m=0 \\ (m,q=1)}}^{q-1} e^{2\pi i \frac{ad}{q} m} + O(q) = \frac{A}{qd} \mu(q) + O(q) = \mu(q) Z_d + O(q).$$

若 $N^{0.8} < d \leqslant N$，則直接就得

$$\tau(d) = 2^{\Omega(d)} = b_0^{\Omega(d) r^{\varepsilon-1} \ln 2} > d^{r^{\varepsilon-1} \ln 2} > e^{0.55 r^{\varepsilon}};\quad 1 < \frac{\tau(d)}{e^{0.55 r^{\varepsilon}}},$$

$$|S_d| \leqslant \sum_{\frac{N-A}{d} < m \leqslant \frac{N}{d}} 1,\ Z_d \leqslant \sum_{\frac{N-A}{d} < m \leqslant \frac{N}{d}} 1,\ S_d - \mu(q) Z_d \ll \sum_{\frac{N-A}{d} < m \leqslant \frac{N}{d}} 1.$$

因之，等式（4）之右邊可以化成

$$\mu(q) R + O(N^{0.8} q + B);\quad R = \sum_{d/P} \mu(d) Z_d, B = \sum_{N^{0.8} < d \leqslant N} \sum_{\frac{N-A}{d} < m \leqslant \frac{N}{d}} \frac{\tau(d)}{e^{0.55 r^{\varepsilon}}}.$$

令 z 跑過區間 $N - A < z \leqslant N$ 中形如 $qx + 1$ 之整數，並設 $f(z) = 1$，運用引理 2, a，則我們即已證明 R 恰好等於與 P 互素的 z 的個數，因而 R 不大於那種 z 值的個數，這種 z 值是和不超過 b_1 且除不盡 q 的素數所成之積互素者．故得（引理 4）

$$R \ll \frac{A(rq)^{2\varepsilon}}{rq}.$$

再，若令 $N_m = \max\left(\frac{N-A}{m}, N^{0.8}\right)$，則我們即得（第一章引理 17,c）

$$B = \sum_{0 < m \leqslant N^{0.2}} \sum_{N_m < d \leqslant \frac{N}{m}} \frac{\tau(d)}{e^{0.55 r^{\varepsilon}}} \ll \sum_{0 < m \leqslant N^{0.2}} \frac{Ar}{m} e^{-0.55 r^{\varepsilon}} \ll \frac{A}{r\sqrt{q}}.$$

因而等式（4）之右邊將

$$\ll \frac{A(rq)^{2\varepsilon}}{r\sqrt{q}}.$$

我們現轉到等式左邊的和數．對於它的那種項，它所對應的 z 值滿足條件 $\mu(z) = 0$ 者，其項的數目 D 將

$$D \ll \sum_{b_0 < p \leqslant \sqrt{N}} \left(\frac{A}{p^2} + 1\right) \ll \frac{A}{b_0} + \sqrt{N} \ll \frac{A}{r\sqrt{q}}.$$

若用字母 k_0 來記 $\Omega(z)$ 關於其餘的那些 z 所取的值之最大者，則由顯然的不等式 $b_0^{k_0} \leqslant N$，我們即得 $k_0 \leqslant r^{\varepsilon}$．因之，由等式（4）即得

$$\sum_{0<k\leqslant k_0} H_k \ll \frac{A(rq)^{2\varepsilon}}{r\sqrt{q}};\quad k_0 \leqslant r^{\varepsilon};\quad H_k = \sum_{N-A<z_k\leqslant N} e^{2\pi i \frac{a}{q} z_k}, \tag{5}$$

於此，z_k 跑過由 k 個大於 b_0 的不同的素因子所成之積.

當 $k>1$，我們現來研究和數

$$L_k = \sum\sum_{N-A<pv\leqslant N} e^{2\pi i \frac{a}{q} pv},$$

於此，p 跑過大於 b_0 之素數，而 v 則跑過由 $k-1$ 個大於 b_0 的不同的素因子所成之積. 和數 L_k 中滿足 $(p,v)=p$ 的項，其和顯然 $\ll D$. 而和數 L_k 中餘下的那些項也正是和數 H_k 中的那些項，但後一和數的每一項在 L_k 中恰好出現 k 次. 因之

$$H_k = \frac{1}{k} L_k + O\left(\frac{A}{r\sqrt{q}}\right).$$

我們現來估計 L_k. 我們將區間 $b_0 < p \leqslant N b_0^{-k+1}$ 分成 $\ll r$ 個形如

$$Y < p \leqslant Y';\qquad 2Y \leqslant Y' \leqslant 3Y \tag{6}$$

之區間，同時又將區間 (6) 分成 $\ll Yb^{-1}$ 個形如

$$U < p \leqslant U+W;\qquad b \leqslant W \leqslant 2b$$

之區間. 令

$$M = \sum_{U<p\leqslant U+W}\ \sum_{\frac{N-A}{p}<v\leqslant\frac{N}{p}} e^{2\pi i \frac{a}{q} pv}.$$

用和數

$$M' = \sum_{U<p\leqslant U+W}\ \sum_{\frac{N-A}{U}<v\leqslant\frac{N}{U}} e^{2\pi i \frac{a}{q} pv}$$

代替 M，所致的誤差顯然將

$$\ll W\frac{NW}{U^2} = \frac{WA}{U}\frac{NW}{AU} \ll \frac{WA}{U}\frac{b_1 b}{b_0} \ll \frac{WA}{Ur^2\sqrt{q}}.$$

但由於 $W \geqslant b$, $AU^{-1} \geqslant b_0^{k-1}\, b_1^{-1} \gg b$, 故對於滿足條件 $0 \leqslant l < q$, $0 \leqslant t < q$, $(l,q)=(t,q)=1$ 之 l 及 t, 關於形如 $qx+l$ 且屬於區間

$$U < p \leqslant U+W$$

之 p 的個數 $\xi(l)$ 及關於形如 $qx+t$ 且屬於區間

$$\frac{N-A}{U} < v \leqslant \frac{N}{U}$$

之 v 的個數 $\eta(t)$，我們有不等式（引理 4）

$$\xi(l) \ll \frac{W(rq)^{2\varepsilon}}{rq}; \qquad \eta(t) \ll \frac{A(rq)^{2\varepsilon}}{Urq}.$$

同時，若當 $(l, q) > 1$ 令 $\xi(l) = 0$，當 $(t, q) > 1$ 令 $\eta(t) = 0$，則有

$$M' = \sum_{l=0}^{q-1} \sum_{t=0}^{q-1} \xi(l)\, \eta(t)\, e^{2\pi i \frac{a}{q} lt}.$$

因之（第一章引理 10, a）

$$M' \ll \frac{WA(rq)^{4\varepsilon}}{Ur^2\sqrt{q}}; \qquad M \ll \frac{WA(rq)^{4\varepsilon}}{Ur^2\sqrt{q}}.$$

同時，和數 L_k 中對應於區間 (6) 之部分將

$$\ll \frac{WA(rq)^{4\varepsilon}}{Ur^2\sqrt{q}} \frac{Y}{b} \ll \frac{A(rq)^{4\varepsilon}}{r\sqrt{q}}.$$

由是卽得

$$L_k \ll \frac{A(rq)^{4\varepsilon}}{r\sqrt{q}}; \qquad H_k \ll \frac{A(rq)^{4\varepsilon}}{kr\sqrt{q}}.$$

據此及不等式

$$L_1 - S \ll b_0 \ll \frac{A}{r\sqrt{q}},$$

由 (5) 卽得我們的定理.

定理 2, b. 設 $1 < H \leqslant e^{r^\varepsilon}$；$\tau = NH^{-1}$,

$$\alpha = \frac{a}{q} + z; \quad (a, q) = 1; \quad 0 < q \leqslant e^{r^{0.5\varepsilon}}; \quad |z| \leqslant \frac{1}{q\tau},$$

$$S = \sum_{p \leqslant N} e^{2\pi i \alpha p}.$$

則有

$$S \ll \frac{N(rq)^{5\varepsilon}}{r\sqrt{q}}.$$

證. 我們將區間 $0 < p \leqslant N$ 分成 $[e^{\sqrt{r}}]$ 個長為 $A = N\,[e^{\sqrt{r}}]^{-1}$ 之區間. 令

$$N_1 - A < p \leqslant N_1 \tag{7}$$

為如是之區間之一. 設 $r_1 = \ln N_1$，卽有

$$N_1 e^{-\sqrt{r_1}} \leqslant A \leqslant N_1; \qquad r - \sqrt{r} \leqslant r_1; \qquad r^{0.5\varepsilon} < r_1^\varepsilon; \qquad 0 < q \leqslant e^{r_1^\varepsilon}.$$

利用簡易變換，可將和數 S 中對應於區間 (7) 之部分表成

$$\sum_{N_1-A<p\leqslant N_1} e^{2\pi i\left(\frac{a}{q}p+zN_1\right)}+O\left(\frac{A^2}{q\tau}\right)$$

之形式,依據定理 2, a, 此將

$$\ll \frac{A(r_1q)^{5\varepsilon}}{r_1\sqrt{q}}+\frac{A^2}{q\tau}\ll\frac{A(rq)^{5\varepsilon}}{r\sqrt{q}}.$$

故得

$$S\ll[e^{\sqrt{r}}]\frac{A(rq)^{5\varepsilon}}{r\sqrt{q}}\ll\frac{N(rq)^{5\varepsilon}}{r\sqrt{q}}.$$

引理 5. 設 $0<c\leqslant\frac{1}{6}$; $0<\sigma\leqslant\frac{1}{3}$; $0\leqslant\gamma\leqslant 1-\sigma$; P 爲所有不大於 N^σ 之素數之積. 若令

$$D=r^{\frac{\ln r}{\ln(1+c)}},$$

則 P 的不大於 N 之因子 d 可以分成 $<D$ 個集合,對於每一個集合存在一個 φ,使得所有屬於這一集合中之值 d 皆滿足不等式

$$\varphi<d\leqslant\varphi^{1+c}.$$

對於某些集合,有 $\varphi\leqslant N^\gamma$; 對於其餘的每一集合則存在一整數 B 及二增加正整數列 (x) 與 (y),其中所有的 x 皆屬於某一個完全屬於區間 $N^\gamma<x\leqslant N^{\gamma+\sigma+c}$ 中的區間 $\varphi_0<x\leqslant\varphi_0^{1+c}$ 內;若從所有乘積 xy 中,我們只取滿足條件 $(x,y)=1$ 的那些數,則我們卽得出所討論的集合中所有之數 d, 每一個取 B 次,且僅這些數可得.

證. 設 τ 爲滿足條件

$$2^{(1+c)^{\tau-1}}\leqslant N^\sigma$$

的最大整數. 則有

$$(1+c)^{\tau-1}\leqslant\frac{r}{3\ln 2};\quad \tau-1\leqslant\frac{\ln r-\ln\ln 8}{\ln(1+c)};\quad \tau<\frac{\ln r}{\ln(1+c)}-1.$$

令 $b=[r]$, 我們現來討論所有不增數列 $t_1,\cdots,t_b$, 這裏的每一 t, 皆是自 $\tau,\cdots,1,0$ 中取出. 設 l_s 爲數列 $t_1,\cdots,t_b$ 中等於 s 的數的個數. 數列 $t_1,\cdots,t_b$ 卽由數目 $l_\tau,\cdots,l_1$ 完全決定; 由是可知,所有的這種數列爲數將 $<D$.

當 $t_j>0$ 時,我們令

$$\varphi_j=2^{(1+c)^{t_j-1}};\qquad F_j=\varphi_j^{1+c}=2^{(1+c)^{t_j}},$$

而當 $t_j=0$ 時,我們令

$$\varphi_j = F_j = 1.$$

所有不超過 N 之 d 皆是 $\leqslant b$ 個素因子之積;否則由

$$2 \cdots (b+2) \leqslant N, \quad \ln 2 + \cdots + \ln(b+2) \leqslant r; \quad \int_1^r \ln x \, dx \leqslant r;$$
$$r \ln r \leqslant 2r - 1,$$

若 c_0 充分大,此乃不可能者. 將數 d 的素因子按從大至小的次序排列,若因子的個數 h 小於 b,則令 $p_{h+1} = \cdots = p_b = 1$,我們卽將 d 表成 $d = p_1 \cdots p_b$ 之形式. 在數列 $t_1, \cdots, t_b$ 中,可以找到唯一的一個數列滿足條件

$$\begin{aligned} &\varphi_j < p_j \leqslant F_j, \quad 當 \quad t_j > 0, \\ &\varphi_j = p_j = F_j, \quad 當 \quad t_j = 0, \end{aligned} \tag{1}$$

我們就說,所討論的 d 與這一數列 $t_1, \cdots, t_b$ 對應. 令 $\varphi = \varphi_1 \cdots \varphi_b$,則有 $\varphi < d \leqslant \varphi^{1+c}$.

假定 $\varphi > N^r$,我們現來討論所有與給定的數列 $t_1, \cdots, t_b$ 對應的 d 所成之集合. 用字母 β 來記滿足條件 $\varphi_1 \cdots \varphi_\beta > N^r$ 之最小整數,則得(若 $\beta = 1$,則可認爲 $\varphi_1 \cdots \varphi_{\beta-1} = 1$)

$$\varphi_1 \cdots \varphi_{\beta-1} \leqslant N^r, \quad \varphi_\beta \leqslant N^\sigma, \quad \varphi_1 \cdots \varphi_\beta \leqslant N^{r+\sigma}, \quad (\varphi_1 \cdots \varphi_\beta)^{1+c} \leqslant N^{r+\sigma+c}.$$

令 $x = p_1 \cdots p_\beta$, $y = p_{\beta+1} \cdots p_b$, $\varphi_0 = \varphi_1 \cdots \varphi_\beta$,則我們卽可看出所有的值 x 皆在區間 $\varphi_0 < x \leqslant \varphi_0^{1+c}$ 內;而此區間則完全屬於區間 $N^r < x \leqslant N^{r+\sigma+c}$ 之內. 又令 $t_{\beta-k_1+1}, \cdots, t_\beta, t_{\beta+1}, \cdots, t_{\beta+k_2}$ 爲所有等於 t_β 之值 t_j. 當 x 與 y 互相無關地跑過所有滿足條件(1)之積,附上條件 $p_1 > \cdots > p_\beta$; $p_{\beta+1} \geqslant \cdots \geqslant p_b$,於此 $p_s \geqslant p_{s+1}$ 是了解成: 當 $p_s > 1$ 時,$p_s > p_{s+1}$,當 $p_s = 1$ 時,$p_s = p_{s+1}$,則乘積 xy 只當 $(x, y) = 1$ 時始等於所討論的集中之一 d 值,此時等式 $xy = d$ 共有 $B = \binom{k_1 + k_2}{k_1}$ 次成立.

引理 6. 設 x 與 y 跑過屬於二增加數列中的正整數; u 與 v 分別跑過由 c_1 及 c_2 個因子所組成的積,其中每一個因子皆各屬於一個由正整數組成的增加數列. 又設

$$\sqrt{N} \leqslant \tau \leqslant N e^{-r^{\varepsilon_0}},$$

$$\alpha = \frac{a}{q} + \frac{\theta}{q\tau}; \quad (a, q) = 1; \quad e^{r^{\varepsilon_0}} \leqslant q \leqslant \tau; \quad \Delta = \sqrt{\frac{1}{q} + \frac{q}{N}};$$

$1 \leqslant U$; $1 \leqslant X$; $N^{0.2} \ll UX \ll \max(N^{0.8}, N\Delta^5)$; $U' \ll U < U'$; $X' \ll X < X'$,

$$f = \min\left(\Delta^{-1}, \left(\frac{1}{UX} + \frac{UX}{N}\right)^{-0.5}\right), \quad K 是正數整, \quad K \ll f^2,$$

$$S=\sum_{k=1}^{K}\left|\sum_{u}\sum_{x}\sum_{y}\sum_{v} e^{2\pi i a k u x y v}\right|,$$

這裏的求和記號是展布於域

$$U<u\leqslant U';\quad X<x\leqslant X';\quad uxyv\leqslant N;\quad (x,y)=1$$

之上. 則有

$$S\ll KN\left(\Delta^{1+\varepsilon}+\left(\frac{1}{UX}+\frac{UX}{N}\right)^{\frac{1}{2}-\varepsilon}\right).$$

證. 我們有

$$S=\sum_{k=1}^{K}\left|\sum_{d}\mu(d)\sum_{u}\sum_{x'}\sum_{y'}\sum_{v} e^{2\pi i a k d^2 u x' y' v}\right|,$$

於此，d 跑過正整數，而當 d 給定時，x' 與 y' 則跑過其爲 d 之倍數的 x 與 y 經 d 除後所得的商；此時，求和記號係展布於域

$$U<u\leqslant U';\quad X<dx'\leqslant X',\quad d^2ux'y'v\leqslant N$$

之上. 但不定方程 $uy'v=z$ 的解的個數不超過 $\tau_{c_1+c_2+1}(z)$，而由第一章引理 17，不等式 $uy'v\leqslant n$ 之解的個數將 $\ll n(\ln n+1)^{c_1+c_2}$； 因之，和數 S 中對應於大於 f 的 d 值之部分將

$$\ll\sum_{d>f}\frac{KN}{d^2}r^{c_1+c_2+1}\ll\frac{KN}{f}r^{c_1+c_2+1}\ll KNf^{-1+\varepsilon},$$

我們於是得

$$S\ll\sum_{d\leqslant f}S_d+KNf^{-1+\varepsilon};\quad S_d=\sum_{k=1}^{K}S_{d,k};$$

$$S_{d,k}=\sum_{u}\sum_{x'}\left|\sum_{y'}\sum_{v} e^{2\pi i a d^2 k u x' y' v}\right|;\ S_d^2\leqslant K\sum_{k=1}^{K}S_{d,k}^2.$$

但不定方程 $ux'=z$ 的解的個數不超過 $\tau_{c_1+1}(z)$，而由第一章引理 17, b,

$$\sum_{\frac{UX}{d}<z\leqslant\frac{U'X'}{d}}(\tau_{c_1+1}(z))^2\ll\frac{UX}{d}r^{c_1^2+2c_1}.$$

因之，

$$S_{d,k}^2\ll\frac{UX}{d}r^{c_1^2+2c_1}\sum_{\frac{UX}{d}<z\leqslant\frac{U'X'}{d}}\left|\sum\sum_{d^2zy'v\leqslant N} e^{2\pi i a d^2 k z y' v}\right|^2\ll$$

$$\ll\frac{UX}{d}r^{c_1^2+2c_1}\sum_{\frac{UX}{d}<z\leqslant\frac{U'X'}{d}}\ \sum\sum_{d^2zy_1'v_1\leqslant N}\ \sum\sum_{d^2zy'v\leqslant N} e^{2\pi i a d^2 k z(y_1'v_1-y'v)}.$$

我們再將求和記號之次序加以改變,顯而易見,

$$y_1'v_1 \leqslant \frac{N}{dUX}; \quad y'v \leqslant \frac{N}{dUX},$$

而當 y_1', v_1, y', v 給定時, z 則跑過區間

$$\frac{UX}{d} < z \leqslant \min\left(\frac{U'X'}{d}, \frac{N}{d^2 y_1' v_1}, \frac{N}{d^2 y' v}\right)$$

中之整數. 因之

$$S_{d,k}^2 \ll \frac{UX}{d} r^{c_1^2+2c_1} \sum\sum_{y_1'v_1 \leqslant \frac{N}{dUX}} \sum\sum_{y'v \leqslant \frac{N}{dUX}} \min\left(\frac{U'X'}{d}, \frac{1}{2\left(ad^2k(y_1'v_1 - y'v)\right)}\right).$$

設 $\psi(t)$ 爲不定方程 $y'v = t$ 的解的數目. 則不定方程 $y_1'v_1 - y'v = s$ 的解的數目等於 $\sum_t \psi(t)\psi(t+s)$,於此, t 跑過所有滿足條件

$$0 < t \leqslant \frac{N}{dUX}; \qquad 0 < t+s \leqslant \frac{N}{dUX}$$

的整數. 由是

$$T_s \leqslant \sqrt{\sum_t (\psi(t))^2 \sum_t (\psi(t+s))^2} \ll \sum_{0 < t \leqslant \frac{N}{dUX}} (\tau_{c_2+1}(t))^2 \ll \frac{N}{dUX} r^{c_2^2+2c_1}.$$

同時,我們有

$$S_{d,k}^2 \ll \frac{N}{d^2} r^{c_1^2+2c_1+c_2^2+2c_2} \sum_{0 \leqslant s \leqslant \frac{N}{dUX}} \min\left(\frac{UX}{d}, \frac{1}{(ad^2ks)}\right),$$

$$S_d^2 \ll \frac{KN}{d^2} r^{c_1^2+2c_1+c_2^2+2c_2} \sum_{k=1}^{K} \sum_{0 \leqslant s \leqslant \frac{N}{dUX}} \min\left(\frac{UX}{d}, \frac{1}{(ad^2ks)}\right). \tag{2}$$

我們先來討論 $N^{0.1} \leqslant q \leqslant N^{0.9}$ 之情形. 我們將區間 $1 \leqslant d \leqslant f$ 中所有之值 d 分入 $\ll r$ 個形如

$$D < d \leqslant D'; \qquad D' \leqslant 2D$$

之區間內.

設 $S(D)$ 爲和數 S 對應於如是之一新區間之部分;則

$$S(D) = \sum_{D < d \leqslant D'} S_d; \qquad (S(D))^2 \leqslant D \sum_{D < d \leqslant D'} |S_d|^2.$$

注意當 d, k, s 跑過滿足條件

$$D < d \leqslant D'; \quad 0 < k \leqslant K; \quad 1 \leqslant s \leqslant \frac{N}{dUX}$$

之値時,不定方程 $d^2 k s = l$ 之解的個數將 $\ll N^{\varepsilon'}$ (第一章引理 17, a),我們即得

$$(S(D))^2 \ll \frac{KN}{D} N^{\varepsilon''} \sum_{0<l\leqslant \frac{2DKN}{UX}} \min\left(\frac{UX}{K}, \frac{1}{(\alpha l)}\right) + \frac{K^2NUX}{D} N^{\varepsilon''},$$

由是,依據第一章引理 8, a (將長爲 $\frac{2\,DKN}{UX}$ 之區間分成 $< \frac{2\,DKN}{UXq} + 1$ 個長$\leqslant q$ 之區間),

$$(S(D))^2 \ll \frac{KN}{D} N^{\varepsilon''} \left(\frac{DKN}{UXq} + 1\right)\left(\frac{UX}{D} + q \ln q\right) + \frac{K^2NUX}{D} N^{\varepsilon''} \ll$$

$$\ll K^2 N^{2+\varepsilon'''} \left(\frac{1}{q} + \frac{1}{UX} + \frac{UX}{N} + \frac{q}{N}\right).$$

由此即不難得出在引理中所說之不等式.

我們再來討論 $q < N^{0.1}$ 之情形. 設 $(d^2, q) = \delta$, $d^2 = d_1 \delta$, $q = q_1 \delta$, $(q_1, k) = \kappa$, $q_1 = q_2 \kappa$, $k = k_1 \kappa$. 則

$$\alpha d^2 k = \frac{a d_1 k_1}{q_2} + \frac{\theta d_1 k_1}{q_2 \tau}; \qquad \frac{d_1 k_1}{\tau} \leqslant \frac{1}{q^2}.$$

因之 (第一章引理 8, a) 不等式 (2) 右邊對應於所取的 k 的部分將

$$\ll \frac{KN}{d^2} q^{\varepsilon'} \left(\frac{N}{dUXq_2} + 1\right)\left(\frac{UX}{d} + q_2\right) \ll \frac{KN}{d^2} q^{\varepsilon'} \left(\frac{N}{d^2 q_2} + \frac{N}{dUX} + \frac{UX}{d}\right);$$

又,對應於具有給定的 κ 的一切 k 之部分將

$$\ll \frac{KN}{d^2} q^{\varepsilon'} \left(\frac{NK}{d^2 q_2 \kappa} + \frac{NK}{dUX\kappa} + \frac{UKX}{d\kappa}\right) \ll \frac{K^2N^2}{d^2} q^{\varepsilon'} \left(\frac{1}{d^2 q_1} + \frac{1}{dUX} + \frac{UX}{dN}\right) \ll$$

$$\ll \frac{K^2N^2}{d^2} q^{\varepsilon'} \left(\frac{1}{q} + \frac{1}{UX} + \frac{UX}{N}\right).$$

由是

$$S_d^2 \ll \frac{K^2N^2}{d^2} q^{\varepsilon''} \left(\frac{1}{q} + \frac{1}{UX} + \frac{UX}{N}\right).$$

而引理中所說之不等式已不難得出.

最後,我們來討論 $q > N^{0.9}$ 之情形 (祗當 $\tau > N^{0.9}$ 時可能). 設 $(d^2 k, q) = \delta$, $d^2 k = d_1 \delta$, $q = q_1 \delta$; 則

$$\alpha d^2 k = \frac{a d_1}{q_1} + \frac{\theta d_1}{q_1 \tau} = \frac{a d_1}{q_1} + \frac{\theta \lambda}{q_1^2}; \quad \lambda = d^2 k / \delta.$$

因之 (第一章引理 8, a),

$$\sum_{0<s\leqslant\frac{N}{dUX}} \min\left(\frac{UX}{d}, \frac{1}{(\alpha d^2 ks)}\right) \ll d^2 k\frac{UX}{d} + q_1 \ln q_1,$$

$$S_d^2 \ll \frac{KN}{d^2}\left(\frac{N}{q}\right)^{\epsilon} Kq \ll \frac{K^2N^2}{d^2}\left(\frac{N}{q}\right)^{\epsilon}\frac{q}{N},$$

由是,引理中所說之不等式已不難得出.

定理 3. 設 $\sqrt{N} \leqslant \tau \leqslant Ne^{-r^{\epsilon_0}}$;

$$\alpha = \frac{a}{q} + \frac{\theta}{q\tau};\quad (a, q) = 1;\quad e^{r^{\epsilon_0}} \leqslant q \leqslant \tau;\quad \Delta = \sqrt{\frac{1}{q} + \frac{q}{N}};\quad f = \Delta^{-1};$$

K 為整數, $0 < K \leqslant f^2$; p 跑過素數,

$$S = \sum_{k=1}^{K}\left|\sum_{p\leqslant N} e^{2\pi i\alpha kp}\right|.$$

則有

$$S \ll KN(\Delta^{1-\epsilon} + N^{-0.2+\epsilon}).$$

證. 設 $2 \leqslant H \leqslant N^{\frac{1}{3}}$; P 為 $\leqslant H$ 的素數 p 之積; Q 為滿足條件 $H < p \leqslant N$ 的素數 p 之積; S_0 為滿足條件 $H^{s_0} < N$ 之最大整數. 對於取值 $s = 1, \cdots, s_0$ 中之一的 s, 令

$$\sum_{\substack{y_1/Q \\ y_1\cdots y_s\leqslant N}} \cdots \sum_{y_s/Q} e^{2\pi i\alpha k y_1\cdots y_s} = W_s, \tag{3}$$

我們有

$$W_s = \sum_{d_1/P}\sum_{\substack{m_1>0 \\ d_1m_1\cdots d_sm_s\leqslant N}} \cdots \sum_{d_s/P}\sum_{m_s>0} \mu(d_1)\cdots\mu(d_s)\, e^{2\pi i\alpha k d_1m_1\cdots d_sm_s}.$$

設 j 為一自然數, D_j 為 j 個不同素數之積. 令

$$S_j = \sum_{D_j/Q} e^{2\pi i\alpha k D_j}.$$

在 (3) 的左邊指數上的諸乘積 $y_1\cdots y_s$ 中,所給的 D_j 出現 s_j 次,因為它的每一個素因子皆可在 $y_1, y_2, \cdots$, 以及 y_s 中出現. 因為諸乘積 $y_1\cdots y_s$ 中有一等於 1, 有 $\ll N^{1+\epsilon}H^{-1}$ 個乘積可為一大於 1 的整數的平方所整除,故由 (3), 即得

$$sS_1 + s^2S_2 + \cdots + s^{s_0}S_{s_0} = W_s + O(N^{1+\epsilon}H^{-1}). \tag{4}$$

現令 $H = N^{0.2}$; 則 $s_0 = 4$. 對 $s = 1, 2, 3, 4$, 由等式 (4) 即得

$$S_1 + S_2 + S_3 + S_4 = W_1 + O(N^{0.8+\epsilon});$$

$$S_1+2S_2+4S_3+8S_4=\frac{W_2}{2}+O(N^{0.8+\varepsilon});$$

$$S_1+3S_2+9S_3+27S_4=\frac{W_2}{3}+O(N^{0.8+\varepsilon});$$

$$S_1+4S_2+16S_3+64S_4=\frac{W_4}{4}+O(N^{0.8+\varepsilon}).$$

因之,

$$S_1=\frac{\Delta_1}{\Delta}W_1-\frac{\Delta_2}{2\Delta}W_2+\frac{\Delta_3}{3\Delta}W_3-\frac{\Delta_4}{4\Delta}W_4+O(N^{0.8+\varepsilon}),$$

於此, Δ_1, Δ_2, Δ_3, Δ_4, 爲行列式

$$\Delta=\begin{vmatrix}1&1&1&1\\1&2&4&8\\1&3&9&27\\1&4&16&64\end{vmatrix}$$

中對應於第一列元素之小行列式. 由是,由於 $S=\sum_{k=1}^{K}|S_1|+O(K\sqrt{N})$,我們卽得

$$S\ll\sum_{k=1}^{K}|W_1|+\sum_{k=1}^{K}|W_2|+\sum_{k=1}^{K}|W_3|+\sum_{k=1}^{K}|W_4|+KN^{0.8+\varepsilon}.$$

我們下面祇限於估計此等式右邊第四被加項,因爲前三個被加項可用同樣的方法估計. 對於每一 $j=1,2,3,4$, 依據引理 5 (當 $\sigma=0.2$), 所有之 d_j 值可以分入 $<D$ 個集合,而所有之值 m_j 則可分入 $\ll r$ 個集合,滿足形如

$$M_j<m_j\leqslant M_j',\qquad M_j'\leqslant 2M$$

的條件. 令

$$T=\sum_{k=1}^{K}\left|\sum_{d_1}\sum_{d_2}\sum_{d_3}\sum_{d_4}\sum_{m_1}\sum_{m_2}\sum_{m_3}\sum_{\substack{m_4\\ d_1d_2d_3d_4m_1m_2m_3m_4\leqslant N}}e^{2\pi i\alpha kd_1d_2d_3d_4m_1m_2m_3m_4}\right|,$$

於此,求和記號係展布於由不等式

$$\varphi^{(1)}<d_1\leqslant F^{(1)};\quad \varphi^{(2)}<d_2\leqslant F^{(2)};\quad \varphi^{(3)}<d_3\leqslant F^{(3)};\quad \varphi^{(4)}<d_4\leqslant F^{(4)},$$
$$F^{(j)}=(\varphi^{(j)})^{1+c}$$

所定義的 d_1, d_2, d_3, d_4, 之四個集合、及由不等式

$$M_1<m_1\leqslant M_1';\quad M_2<m_2\leqslant M_2';\quad M_3<m_3\leqslant M_3';\quad M_4<m_4\leqslant M_4'$$

所定義的 m_1, m_2, m_3, m_4, 之四個集合. 我們只須考慮

$$M_1 M_2 M_3 M_4 \varphi^{(1)} \cdots \varphi^{(4)} < N^{0.8}$$

之情形,蓋在另一種情形,則有(ε 可取得任意小)

$$T \ll KNN^{-0.2+\varepsilon}.$$

先設 $M_1 M_2 M_3 M_4 \leqslant N^{0.4}$. 設 t 為滿足條件 $M_1 M_2 M_3 M_4 \varphi^{(1)} \cdots \varphi^{(t)} > N^{0.4}$ 之最小整數;顯然 $t \geqslant 1$. 用等式 $M_1 M_2 M_3 M_4 \varphi^{(1)} \cdots \varphi^{(t-1)} N^{\gamma} = N^{0.4}$ 定義 γ, 我們有 $\varphi^{(t)} > N^{\gamma}$. 令 $u = m_1 m_2 m_3 m_4 d_1 \cdots d_{t-1}$, $v = d_{t+1} \cdots d_4$.

依據引理 5, 存在着正整數 B 及兩個增加正整數列 (x) 及 (y), 滿足條件 $N^{\gamma} < x \leqslant N^{\gamma+0.2+\varepsilon}$,使得當我們從乘積 xy 中只取滿足條件

$$xy \leqslant N; \quad (x, y) = 1$$

之數,則即得所有之數 d_t, 各取 B 次. 我們將值 u 分成 $\ll r$ 個集合,其中每一個集合祇包含滿足條件 $U < u \leqslant U'$, $U' \leqslant 2U$ 之值; 同樣,我們將值 x 分成 $\ll r$ 個集合,其中每一個集合祇包含滿足條件 $X < x \leqslant X'$, $X' \leqslant 2X$ 之值. 若 T_1 是和數 T 中對應於區間 $U < u \leqslant U'$, $X < x \leqslant X'$ 的部分,則由引理 6, 我們有

$$T_1 \ll KN\left(\Delta^{1-\varepsilon} + \left(\frac{1}{UX} + \frac{UX}{N}\right)^{0.5-\varepsilon}\right),$$

由是,由於(ε 可取得任意小)

$$\frac{1}{UX} \ll \frac{1}{M_1 M_2 M_3 M_4 \varphi^{(1)} \cdots \varphi^{(t-1)} N^{\gamma}} \ll N^{-0.4},$$

$$\frac{UX}{N} \ll \frac{M_1 M_2 M_3 M_4 F^{(1)} \cdots F^{(t-1)} N^{\gamma+0.2+\varepsilon}}{N} \ll N^{-0.4+\varepsilon},$$

我們有

$$T_1 \ll KN(\Delta^{1-\varepsilon'} + N^{-0.2+\varepsilon'}); \quad T \ll KN(\Delta^{1-\varepsilon''} + N^{-0.2+\varepsilon''}).$$

我們現來討論 $M_1 M_2 M_3 M_4 > N^{0.4}$ 之情形. 不失其普遍性,可以假定 M_4 爲所有 M_1, M_2, M_3, M_4 中之最大者.

我們先設 $M_4 \leqslant N^{0.2}$. 設 t 爲滿足條件 $M_1 \cdots M_t > N^{0.4}$ 之最小數. 則若令 $u = m_1 \cdots m_t$, $v = m_{t+1} \cdots m_4 d_1 d_2 d_3 d_4$, $U = M_1 \cdots M_t$, 我們有 $N^{0.4} < U \ll N^{0.6}$, $U < u \leqslant 16U$. 因之,運用引理 6(取 $x = y = 1$),則得

$$T \ll KN\left(\Delta^{1-\varepsilon} + \left(\frac{1}{U} + \frac{U}{N}\right)^{0.5-\varepsilon}\right) \ll KN(\Delta^{1-\varepsilon} + N^{-0.2+\varepsilon}).$$

我們現設 $M_4 > N^{0.2}$. 若此時有 $N^{0.1} \leqslant q \leqslant N^{0.9}$, 或在條件 $q < N^{0.1}$, $q > N^{0.9}$ 之一之下, 有 $M_4 > N\Delta^5$, 則不定方程 $k d_1 d_2 d_3 d_4 m_1 m_2 m_3 = z$ 之解的個數將

$\ll \Delta^{-\varepsilon}$. 因之（第一章引理 8, b）

$$T \ll \Delta^{-\varepsilon} \sum_{0<z<\frac{KN}{M_4}} \min\left(\frac{KN}{z}, \frac{1}{2(\alpha z)}\right) \ll KN\Delta^{-\varepsilon'}\left(\frac{q}{N} + \frac{1}{q} + N^{-0.2}\right) \ll$$

$$\ll KN\left(\Delta^{1-\varepsilon''} + N^{-0.2+\varepsilon''}\right).$$

最後，若在條件 $q < N^{0.1}$, $q > N^{0.9}$ 之一之下有 $M_4 \leqslant N\Delta^5$, 則運用引理 6, 置 $u = m_4$, $v = d_1 d_2 d_3 d_4 m_1 m_2 m_3$, 卽得 $(x = y = 1)$

$$T \ll KN\left(\frac{1}{q} + \frac{1}{N^{0.2}} + \Delta^5 + \frac{q}{N}\right)^{0.5-\varepsilon} \ll KN\Delta^{1-\varepsilon'}.$$

從上所證，卽得我們的定理.

第　十　章

哥　特　巴　赫　問　題

在本章裏，我要來解決哥特巴赫關於任何 $\geqslant c_0$ (c_0 充分大)的奇數 N 可以表成三個素數之和的問題，並導出表法的種數的漸近公式.

這裏所運用的方法也有可能用來解決更一般的堆壘素數問題；例如，對於整數 $n > 1$，將整數 $N \geqslant c_0$ 表成

$$N = p_1^n + \cdots + p_s^n$$

的形式的問題(素變數的華林問題). 但我不在這裏來討論這類一般性的問題.

爲要解决哥特巴赫問題，我現來研究一個積分，它與哈代及李托伍德爲了同一目的所曾指出的積分相似. 亦如第四章及第七章，我將積分區間分成基本區間及餘區間. 關於對應於基本區間的那部分積分之研究，在我 1937 年論哥特巴赫問題的工作出現之前不久，英國的學者們卽曾做出了一般性的方法[以佩治 (Page) 關於算術數列中的素數分佈的結果爲基礎的埃斯特爾曼 (Estermann) 方法]，這種方法，旣可用於哥特巴赫問題，也可以用於更一般的素變數的堆壘問題. 這種方法是以近代的 L 級數論爲基礎. 在這裏，關於這一部分積分的研究，我利用了簡化過的佩治的結果(引理 1) 結合着布朗 (Brun) 方法的某些基本成分(第九章定理 2). 對於與餘區間對應的那部分積分的估值，我只用我自己的一般性方法.

專用記號. 在本章裏，p 常表示素數，c_0 爲一充分大的數，N 爲 $\geqslant c_0$ 的整數；最後，$\ln N = r$.

引理 1（佩治）. 設 ε_0 爲正數，c_1 與 c 爲任意大的數．則在算術數列

$$qx+l;\ 0<q\leqslant r^{c_1};\ (q,l)=1;\ 0\leqslant l<q$$

中，其不超過 N 的素數的個數 $\pi(N,q,l)$ 可以表成公式

$$\pi(N,q,l)=\frac{1}{q_1}\int_2^N\frac{dx}{\ln x}+H,\quad q_1=\varphi(q),$$

於此，對於一切 q，可能除去一列特殊的 q，其爲某一滿足條件

$$q_0\geqslant r^{2-\varepsilon_0}$$

的 $q=q_0$ 的倍數者，之外，我們有不等式

$$H\ll\frac{Nr^{-c}}{q_1 r}.$$

證. 此定理的證明，我不能放在這裏．它是佩治[1]作出的．證明所根據的是一般 L 級數論，這是由狄里克萊、黎曼、阿達碼、窪雷·布散、哈代-李托伍德、蘭道等人的勞力所研究出來的．

引理 2. 設 $\tau=Nr^{-c}$，於此，$c\geqslant 4$，又設

$$R=\int_{-1/\tau}^{1/\tau}(J(z))^3e^{-2\pi izN}dz;\ J(z)=\int_2^N\frac{e^{2\pi izx}}{\ln x}dx.$$

則有

$$R=\frac{N^2}{2r^3}+O\left(\frac{N^2}{r^4}\right).$$

證. 將積分 R 與積分

$$R_0=\int_{-\frac{1}{2}}^{\frac{1}{2}}(I(z))^3e^{-2\pi izN}dz;\quad I(z)=\int_2^N\frac{e^{2\pi izx}}{r}dx$$

比較，我們有

$$R-R_0=\int_{-1/\tau}^{1/\tau}((J(z))^3-(I(z))^3)e^{-2\pi izN}dz+\left(\int_{-1/\tau}^{1/\tau}(I(z))^3e^{-2\pi izN}dz-R_0\right).$$

但在右邊第一項中的被積函數，我們有

---

1) *Proc. London Math. Soc.* (2),39, 1935, 116—141 頁.

$$|J(z)-I(z)|<\int_2^N\left(\frac{1}{\ln x}-\frac{1}{r}\right)dx \ll \frac{N}{r^2}.$$

因之,此第一項(第一章引理 14,b) 將

$$\ll \int_{-1/\tau}^{1/\tau}\frac{N}{r^2}3Z^2\,dz \ll \int_0^{N^{-1}}\frac{N^3}{r^4}\,dz+\int_{N^{-1}}^{1/\tau}\frac{N}{r^4z^2}\,dz \ll \frac{N^2}{r^4}.$$

又右邊第二項

$$\ll \int_{1/\tau}^{\frac12} Z^3\,dz \ll \int_{1/\tau}^{\frac12}\frac{dz}{z^3r^3} \ll \frac{N^2}{r^{11}};$$

故 $R-R_0 \ll N^2\gamma^{-4}$. 此外,假定

$$R'=\int_{-\frac12}^{\frac12}(S(z))^3e^{-2\pi izN}\,dz;\ S(z)=\sum_{x=3}^{N}\frac{e^{2\pi izx}}{r},$$

我們卽有(第一章引理 13)

$$I(z)-S(z)\ll r^{-1};$$

$$R_0-R'\ll\int_0^{\frac12}Z^2r^{-1}\,dz=\int_0^{N^{-1}}\frac{N^2}{r^3}\,dz+\int_{N^{-1}}^{\frac12}\frac{dz}{r^3z^2}\ll\frac{N}{r^3}.$$

因之, $R-R'\ll N^2r^{-4}$. 但 r^3R' 顯然是表示將數 N 表成

$$N=x_1+x_2+x_3$$

的形式的表法個數,於此, x_1, x_2, x_3 是大於 2 的整數. 對每一 $x_1=3, 4, \cdots, N-6$, 等式 $x_2+x_3=N-x_1$ 有 $N-x_1-5$ 次得以實現,故

$$r^3R'=\sum_{x_1=3}^{N-6}(N-x_1-5)=\frac{(N-7)(N-8)}{2}=\frac{N^2}{2}+O(N),$$

由是,我們的引理卽已證明.

定理. 將奇正數 N 表成三個素數之和

$$N=p_1+p_2+p_3$$

的形式的表法個數 $I(N)$ 可以寫成公式

$$I(N)=\frac{N^2}{2r^3}S(N)+O\left(\frac{N^2}{r^{3.5-\varepsilon}}\right),$$

於此,

$$S(N)=\prod_p\left(1+\frac{1}{(p-1)^3}\right)\prod{}''\left(1-\frac{1}{p^2-3p+3}\right),$$

$\prod_p$ 係展布於所有的素數，而 $\prod''$ 則僅展布於數目 N 的素因子. 此外，

$$S(N) > 0.6.$$

推論(哥特巴赫定理). 存在一數 c_0，使得所有奇數 $N \geqslant c_0$ 皆可表成三個素數之和

$$N = p_1 + p_2 + p_3$$

的形式.

證. 設 $\tau = N r^{-14}$，我們有(第一章引理 4)

$$I(N) = \int_{-\tau^{-1}}^{-\tau^{-1}+1} S_\alpha^3 e^{-2\pi i\alpha N} d\alpha;\ S_\alpha = \sum_{p \leqslant N} e^{2\pi i\alpha p}.$$

包含所有形如

$$\alpha = \frac{a}{q} + z;\quad (a, q) = 1;\quad -\tau^{-1} \leqslant z \leqslant \tau^{-1};\quad 0 < q \leqslant r^3$$

的 α 的區間名爲基本區間；自區間 $-\tau^{-1} \leqslant \alpha \leqslant -\tau^{-1} + 1$ 中除出基本區間後留下之區間名爲餘區間. 依據第一章引理 7，所有餘區間中之 α 皆可表成

$$\alpha = \frac{a}{q} + z;\quad (a, q) = 1;\quad -\frac{1}{q\tau} \leqslant z \leqslant \frac{1}{q\tau};\quad r^3 < q \leqslant \tau$$

的形式. 不難看出，當 N 充分大時，對應於不同數對 a 與 q 之基本區間不可能包含共同的 α 值. 實際上，由

$$\frac{a}{q} + z = \frac{a_1}{q_1} + z_1;\quad \frac{a}{q} \gtrless \frac{a_1}{q_1};\quad |z| \leqslant \frac{1}{\tau};\quad |z_1| \leqslant \frac{1}{\tau}$$

就會得出

$$\left|\frac{aq_1 - a_1 q}{qq_1}\right| \leqslant \frac{2}{\tau};\quad \frac{1}{qq_1} \leqslant \frac{2}{\tau};\quad N \leqslant 2r^{20}.$$

對應於所說的將積分區間分成基本區間及餘區間的分法，積分 $I(N)$ 卽被分成兩項之和

$$I(N) = I_1(N) + I_2(N).$$

1. $I_2(N)$ 的估値. 依據第九章定理 1，當 $q > r^{14}$ 時，有

$$S_\alpha \ll N r^{4.5}\left(\sqrt{\frac{1}{q} + \frac{q}{N}} + e^{-0.5\sqrt{r}}\right) \ll N r^{-2.5},$$

而依第九章定理 2, b，當 $r^3 < q \leqslant r^{14}$ 時有

$$S_\alpha \ll N r^{-2.5+\varepsilon_1}.$$

因之(參看第四章之 3.)

$$I_2(N) \ll N r^{-2.5+\varepsilon_1} \int_0^1 |S_\alpha|^2 \, d\alpha =$$

$$= N r^{-2.5+\varepsilon_1} \int_0^1 \sum_{p' \leqslant N} \sum_{p \leqslant N} e^{2\pi i \alpha (p-p')} \, d\alpha \ll N^2 r^{-3.5+\varepsilon_1}.$$

2. 與不算爲特殊的 q 値對應的基本區間. 任給一 ε_0, 並令 $c_1 = 3$, $c = 48$, 則對引理 1 中所說的 H, 可能除去一列特殊的 q, 其爲某一滿足條件

$$q_0 \geqslant r^{2-\varepsilon_0}$$

的 $q = q_0$ 的倍數者,之外,我們有

$$H \ll \frac{N r^{-49}}{q_1}.$$

我們現來研究積分 $I_1(N)$ 中對應於包有分數 $\frac{a}{q}$ 的部分 $I_{a,q}$, 這裏的分母 q 不算在特殊者之內,且滿足條件 $q \leqslant r^3$. 在如是之區間中任取一 α, 我們將和數 S_α 分成 $[r^{31}]$ 個形如

$$S_{\alpha,N_1} = \sum_{N_1 - A < p \leqslant N_1} e^{2\pi i \left(\frac{a}{q}+z\right) p}; \quad A = N [r^{31}]^{-1}$$

之和. 對於這和數中的項, $|zp - zN_1| \leqslant zA$; 又這種項的數目(引理 1, 令 $q=1$) 將 $\ll A r^{-1}$, 而 $zAAr^{-1} \ll Ar^{-18}$. 因之

$$S_{\alpha,N_1} = e^{2\pi i z N_1} \sum_{N_1 - A < p \leqslant N_1} e^{2\pi i \frac{a}{q} p} + O(Ar^{-18}).$$

但當滿足條件 $0 \leqslant l < q$, $(l, q) = 1$ 的 l 給定時, 區間 $N_1 - A < p \leqslant N_1$ 中形如 $qx + l$ 的素數 p 的個數可以表成公式

$$\frac{1}{q_1} \int_{N_1 - A}^{N_1} \frac{dx}{\ln x} + O\left(\frac{Ar^{-18}}{q_1}\right);$$

因之

$$S_{\alpha,N_1} = \sum_l e^{2\pi i \frac{a}{q} l} \frac{1}{q_1} \int_{N_1 - A}^{N_1} \frac{e^{2\pi i z N_1}}{\ln x} dx + O(Ar^{-18}).$$

再,我們有

$$\sum_l e^{2\pi i \frac{a}{q} l} = \mu(q); \ |zN_1 - zx| \leqslant |z| \, A; \frac{1}{q_1} \int_{N_1 - A}^{N_1} \frac{|z| \, A}{\ln x} dx \ll \frac{|z| A^2}{q_1 r} \ll \frac{Ar^{-18}}{q_1};$$

$$S_{a,N_1}=\int_{N_1-A}^{N_1}\frac{e^{2\pi izx}}{\ln x}dx+O(Ar^{-18});$$

$$S_a=\frac{\mu(q)}{q_1}J(z)+O(Nr^{-18});\ J(z)=\int_2^N\frac{e^{2\pi izx}}{\ln x}dx.$$

但(第一章引理 14, b)

$$\frac{1}{q_1}J(z)\ll\frac{Z}{q_1};\ \frac{Z}{q_1}\gg\frac{\tau r^{-1}}{q_1}\gg Nr^{-18};\ S_a^3-\frac{\mu(q)}{q_1^3}(J(z))^3\ll\frac{Z^2}{q_1^2}Nr^{-18};$$

$$I_{a,q}-\int_{-\tau^{-1}}^{\tau^{-1}}\frac{\mu(q)}{q_1^3}(J(z))^3e^{-2\pi i\left(\frac{a}{q}+z\right)N}dz\ll\int_0^{\tau^{-1}}Z^2q_1^{-2}Nr^{-18}dz\ll$$

$$\ll Nr^{-18}q_1^{-2}\left(\int_0^{N^{-1}}N^2r^{-2}dz+\int_{N^{-1}}^{\tau^{-1}}\frac{dz}{r^2z^2}\right)\ll N^2r^{-20}q_1^{-2}.$$

對於給定的 q，就數列 $0,1,\cdots,q-1$ 中所有與 q 互素的 a 求和，並注意這些 a 值關於模 q 依某種次序與 $-a$ 所取之值同餘，我們卽得

$$\sum_a I_{a,q}=G(q)R+O(N^2r^{-20}q_1^{-1}),$$

$$G(q)=\frac{\mu(q)}{q_1^3}\sum_a e^{2\pi i\frac{a}{q}N};\ R=\int_{-\tau^{-1}}^{\tau^{-1}}(J(z))^3e^{-2\pi izN}dz.$$

由是，由引理 2 及不等式 $|G(q)|\leqslant q_1^{-2}$，我們易得

$$\sum_a I_{a,q}=\frac{N^2}{2r^3}G(q)+O\left(\frac{N^2}{r^4q_1^2}\right).$$

3. 對應於特殊 q 値之基本區間. 現設 q 屬於特殊者之內. 我們有

$$I_{a,q}=\int_{-\tau^{-1}}^{\tau^{-1}}\sum_{p'\leqslant N}\sum_{p''\leqslant N}\sum_{p'''\leqslant N}e^{2\pi i\left(\frac{a}{q}+z\right)(p'+p''+p'''-N)}dz.$$

令 $D=[r^{33}]$，則 $A=ND^{-1}$;

$$I_{a,q}=\sum_{s'=1}^{D}\sum_{s''=1}^{D}\sum_{s'''=1}^{D}I'_{a,q},$$

於此，

$$I'_{a,q}=\int_{-\tau^{-1}}^{\tau^{-1}}\sum_{(s'-1)A<p'\leqslant s'A}\ \sum_{(s''-1)A<p''\leqslant s''A}\ \sum_{(s'''-1)A<p'''\leqslant s'''A}e^{2\pi i\left(\frac{a}{q}+z\right)(p'+p''+p'''-N)}dz.$$

將乘積 $zs'A,\ zs''A,\ zs'''A$ 分別代替 $zp',\ zp'',\ zp'''$，則除 $\ll A^4r^{-3}\tau^{-2}\ll N^2r^{-8}D^{-3}$ 之誤差外，積分 $I'_{a,q}$ 等於乘積 UW，於此

$$U = \sum_{(s'-1)A<p'\leqslant s'A} \sum_{(s''-1)A<p''\leqslant s''A} \sum_{(s'''-1)A<p'''\leqslant s'''A} e^{2\pi i\frac{a}{q}(p'+p''+p'''-N)},$$

$$W = \int_{-\tau^{-1}}^{\tau^{-1}} e^{2\pi iz(s'+s''+s'''-D)A}\,dz.$$

但(第九章定理 2, a)

$$U \ll \frac{A^3 r^{\varepsilon_2}}{r^3 q^{1.5}};\ W \ll \min\left(\frac{1}{\tau}, \frac{1}{|s'+s''+s'''-D|A}\right).$$

此外，對於給定的整數 $h \ll D$, $s'+s''+s'''-D=h$ 的解的個數將 $\ll D^2$. 因之(2. 中之記號)

$$I_{a,q} \ll \frac{N^2}{r^8} + \frac{A^3 r^{\varepsilon_2}}{r^3 q^{1.5}} D^2\left(\frac{1}{\tau} + \sum_{h=1}^{2D}\frac{1}{hA}\right) \ll \frac{N^2 r^{\varepsilon_3}}{r^3 q^{1.5}};\ \sum_a I_{a,q} \ll \frac{N^2 r^{\varepsilon_3}}{r^3 q^{0.5}}.$$

由是，由於 $N^2 r^{-3} G(q) \ll N^2 r^{-3} q_1^{-2}$, 爲了劃一起見，我們可以寫

$$\sum_a I_{a,q} = \frac{N^2}{2r^3} G(q) + O\left(\frac{N^2 r^{\varepsilon_3}}{r^3 q^{0.5}}\right).$$

4. $I(N)$ 的初步公式. 我們有(2. 3. 及 1.)

$$I_1(N) - \sum_{q\leqslant r^3}\frac{N^2}{2r^3}G(q) \ll \sum_{q\leqslant r^3}\frac{N^2}{r^4 q_1^2} + \sum_{s\leqslant r^3 q_0^{-1}}\frac{N^2 r^{\varepsilon_3}}{r^3 (q_0 s)^{0.5}} \ll$$

$$\ll \frac{N^2}{r^4} + \frac{N^2 r^{\varepsilon_3}}{r^3\sqrt{q_0}}\sqrt{\frac{r^3}{q_0}} \ll \frac{N^2 r^{\varepsilon_3}}{r^{3.5}};\quad \sum_{q>r^3}\frac{N^2}{2r^3}G(q) \ll \sum_{q>r^3}\frac{N^2}{r^3 q_1^2} \ll \frac{N^2}{r^4};$$

$$I(N) = \frac{N^2}{2r^3} S(N) + O\left(\frac{N^2 r^{\varepsilon}}{r^{3.5}}\right);\ S(N) = \sum_{q=1}^{\infty} G(q).$$

5. $S(N)$ 的轉換與研究. 我們現來研究級數 $S(N)$. 不難證明，對於兩兩互素的正數 $q_1, \cdots, q_k$, 我們有

$$G(q_1)\cdots G(q_k) = G(q_1\cdots q_k). \tag{1}$$

欲明此，祇須考察 $k=2$ 的情形即可. 令 $\varphi(q_1) = q_{1,1}$, $\varphi(q_2) = q_{2,1}$, 我們有

$$G(q_1)\,G(q_2) = \frac{\mu(q_1)\,\mu(q_2)}{q_{1,1}^3\, q_{2,1}^3} \sum_{\substack{0\leqslant a_1<q_1\\(a_1,q_1)=1}} \sum_{\substack{0\leqslant a_2<q_2\\(a_2,q_2)=1}} e^{2\pi i\left(\frac{a_1}{q_1}N+\frac{a_2}{q_2}N\right)} =$$

$$= \frac{\mu(q_1)\,\mu(q_2)}{(q_{1,1}\,q_{2,1})^3}\sum_{a_1}\sum_{a_2} e^{2\pi i\frac{a_1q_2+a_2q_1}{q_1q_2}N} = G(q_1\,q_2),$$

因爲 $\mu(q_1)\mu(q_2)=\mu(q_1q_2)$，$q_{1,1}q_{2,1}=\varphi(q_1q_2)$ 及 $a_1q_2+a_2q_1$ 跑過模 q_1q_2 的一既約剩餘系.

由於 $G(q)\ll q_1^{-2}$，故級數 $S(N)$ 絕對收斂. 級數

$$\xi_p=1+G(p)+G(p^2)+\cdots$$

也絕對收斂,因爲它的項皆包含在 $S(N)$ 內. 運用 (1)，當 $x>2$ 時,我們有

$$\prod_{p\leqslant x}\xi_p=\sum_{q\leqslant x}G(q)+\sum_{q>x}{}'G(q),$$

於此，$\sum'$ 係展布於不爲 $>x$ 之素數所除盡的 q. 由於 $S(N)$ 絕對收斂，故當 x 無限增大時,右邊前一項趨於 $S(N)$；而第二項則趨於零. 因之,若用記號 $\prod\limits_p$ 來記展布於所有素數之上的乘積,我們卽有

$$S(N)=\prod_p\xi_p.$$

但當 $s>1$ 時 $G(p^s)=0$，此外,顯而易見,

$$G(p)=\begin{cases}\dfrac{1}{(p-1)^3},\text{若 } N \text{ 不爲 } p \text{ 除盡},\\[2ex] \dfrac{-1}{(p-1)^2};\text{若 } N \text{ 能爲 } p \text{ 除盡}.\end{cases}$$

故得

$$S(N)=\prod{}'\left(1+\frac{1}{(p-1)^3}\right)\prod{}''\left(1-\frac{1}{(p-1)^2}\right),\tag{2}$$

於此，$\prod'$ 係展布於除不盡 N 之 p 而 $\prod''$ 則展布於除得盡 N 之 p. 但我們有

$$\prod{}'\left(1+\frac{1}{(p-1)^3}\right)>1;\ \prod{}''\left(1-\frac{1}{(p-1)^2}\right)>\prod_p\left(1-\frac{1}{p^2}\right)>\frac{6}{\pi^2}>0.6,$$

因爲在 Π'' 中,由於 N 爲奇,故只包含奇素數,因而常有 $p_1-1\geqslant p$，此處的 p 是與 p_1 最接近且小於 p_1 的素數. 因而我們眞正有 $S(N)>0.6$.

等式 (2) 可以改寫成

$$S(N)=\prod_p\left(1+\frac{1}{(p-1)^3}\right)\prod{}''\frac{1-\dfrac{1}{(p-1)^2}}{1+\dfrac{1}{(p-1)^3}}=$$

$$=\prod_p\left(1+\frac{1}{(p-1)^3}\right)\prod{}''\left(1-\frac{\dfrac{1}{(p-1)^2}+\dfrac{1}{(p-1)^3}}{1+\dfrac{1}{(p-1)^3}}\right),$$

這已經容易化成定理的陳述中所說的形式.

第　十　一　章

函數 αp 所取的值底分數部分之分佈

在本章裏,我們將運用第九章的結果來解決函數 αp, 當 p 跑過不大於 N 的素數時,它所取的值底分數部分之分佈問題.

這裏所用的方法有可能用於一般性的問題,即當 $f(p)$ 爲高於一次的整多項式及 $f(p)$ 爲依某種意義而言可以用整多項式去密切逼近的函數時,其所取的值底分數部分之分佈問題. 但我們在這裏不來涉及這些問題.

專用記號. 在本章裏, p 常表示素數; N 記 $\geqslant c_0$ 之整數, c_0 充分大. 此外,並設

$$r = \ln N; \quad \pi(N) = \sum_{p \leqslant N} 1 .$$

定理. 設 $\sqrt{N} \leqslant \tau \leqslant N e^{-r^{\varepsilon_0}}$; α 爲實數,

$$\alpha = \frac{a}{q} + \frac{\theta}{q\tau}; \quad (a, q) = 1; \quad e^{r^{\varepsilon_0}} \leqslant q \leqslant \tau;$$

$0 < \beta < 1$; H 爲滿足條件 $p \leqslant N$, $\{\alpha p\} < \beta$ 的素數的個數. 則

$$H = \beta\pi(N) + O(N\gamma); \quad \gamma = \left(\frac{1}{q} + \frac{q}{N}\right)^{\frac{1}{2}-\varepsilon} + N^{-0.2+\varepsilon} .$$

證. 令

$$\varepsilon_1 = \frac{1}{2}\varepsilon, \ \Delta = \left(\frac{1}{q} + \frac{q}{N}\right)^{\frac{1}{2}-\varepsilon_1} + N^{-0.2+\varepsilon_1}; \ K_1 = [\Delta^{-2}]; \ S_m = \sum_{p \leqslant N} e^{2\pi i m \alpha p} .$$

則依第九章定理 3, 對於任意整數 $K \leqslant K_1$, 令

$$U_K = \sum_{m \leqslant K} |S_m| ,$$

則有

$$U_K \ll KN\Delta .$$

當 $\Delta \geqslant 0.25$ 時,定理顯然成立; 因之,我們只考慮 $\Delta < 0.25$ 之情形. 任取實數 A 與 B 滿足條件 $0 \leqslant B - A \leqslant 1 - 2\Delta$, 我們現來考慮第一章引理 12 中取設的以 1 爲週期的函數 $\psi(z)$, 此時假定

$$r = 1, \quad \alpha + \frac{1}{2}\Delta = A, \quad \beta - \frac{1}{2}\Delta = B .$$

於是，我們有

$$\psi(\alpha p)=1,\ 若\ A\leqslant \alpha p\leqslant B\ (\mathrm{mod}\ 1);$$

$$0\leqslant\psi(\alpha p)\leqslant 1,若\ A-\Delta\leqslant\alpha p\leqslant A\ (\mathrm{mod}\ 1),或\ B\leqslant\alpha p\leqslant B+\Delta(\mathrm{mod}\ 1);$$

$$\psi(\alpha p)=0,若\ B+\Delta\leqslant\alpha p\leqslant A-\Delta+1\ (\mathrm{mod}\ 1);$$

$$\psi(\alpha p)=(B-A+\Delta)+\sum_{m=1}^{\infty}(a_m\cos 2\pi m\alpha p+b_m\sin 2\pi m\alpha p), \tag{1}$$

於此,若用等式

$$h_m=\frac{1}{m},\ 若\ m\leqslant\frac{1}{\Delta};\quad h_m=\frac{1}{\Delta m^2},\ 若\ m>\frac{1}{\Delta}$$

定義 h_m，我們即常有

$$a_m\ll h_m,\ b_m\ll h_m.$$

由 (1)，即得

$$\sum_{p\leqslant N}\psi(\alpha p)=\pi(N)(B-A+\Delta)+\sum_{m=1}^{\infty}(a_m S'_m+b_m S''_m),$$

於此，S' 與 S'' 係由等式 $S_m=S'_m+iS''_m$ 所定義. 因之

$$\sum_{m=1}^{\infty}(a_m S'_m+b_m S''_m)\ll\sum_{m=1}^{\infty}h_m|S_m|=\sum_{m\leqslant K_1}h_m|S_m|+\sum_{m>K_1}h_m|S_m|.$$

由是,試注意對於任何整數 $m\geqslant 1$,

$$0<h_m-h_{m+1}\ll\frac{1}{m^2},$$

我們即有

$$\begin{aligned}\sum_{m\leqslant K_1}h_m|S_m|&=h_1U_1+h_2(U_2-U_1)+h_3(U_3-U_2)+\cdots+\\&+h_{K_1}(U_{K_1}-U_{K_1-1})=U_1(h_1-h_2)+U_2(h_2-h_3)+\cdots+\\&+U_{K_1-1}(h_{K_1-1}-h_{K_1})+h_{K_1}U_{K_1}\ll N\Delta\ln K_1+N\Delta\ll N\gamma.\end{aligned}$$

注意常有 $|S_m|\ll N$，我們亦得

$$\sum_{m>K_1}h_m|S_m|\ll\sum_{m>K_1}\frac{N}{\Delta m^2}\ll\frac{N}{\Delta K_1}\ll N\Delta\ll\Delta\gamma.$$

因之,

$$\sum_{p\leqslant N}\psi(\alpha p)=\pi(N)(B-A)+O(N\gamma).$$

由是,依據如在證明第八章定理時所進行之討論,我們的定理已經不難得出.

參 考 文 獻

[1] Landau, E., *Vorlesungen über Zahlentheorie*, I. Leipzig, 1927.

[2] Mordell, L. J., On a sum analogous to a Gauss's sum. *Quart. Journ. Math., Oxford Series*, 1932, т. 3.

[3] Hua Loo-Keng, Аддитивная теория простых чисел. *Тр. Матем. ин-та им. В. А. Стеклова АН СССР*, 1947, т. XXII.

[4] Виноградов И. М. О распределении степенных вычестов и невычетов. *Журн. Физико-матем. об-ва при Перм. ун-те*, 1918, Вып. 1; 選集 54 頁.

[5] Виноградов, И. М. Уточнение метода оценки сумм с простыми числами. *Изв. АН СССР, серия матем.*, 1943, т. 7; 選集 217 頁.

[6] Davenport H., On character sums in finite fields. *Acta Math.*, 1939, т. 71.

[7] Виноградов, И. М., Аналитическое доказательство теоремы о распределении дробных частей целого многочлена. *Изв. АН СССР*, 1927, т. 21, № 7/8; 選集 109 頁.

[8] Линник, Ю. В., О суммах Вейля. *Докл. АН СССР*, 1942, т. 34 № 7.

[9] Чудаков, Н. Г., О Нулях L-функции Дирихле. *Матем, сборник*, 1936, 1(43), № 4.

[10] Van der Corput J. G., Zahlentheoretische Abschätzungen mit Anwendung auf Gitterpunktprobleme. *Math. Zschr.*, 1923, т. 17.

[11] Виноградов, И. М. О распределении дробных долей значений функций двух переменных. *Изв. Ленингр. политехн. ин-та*, 1929, т. 33; 選集 119 頁.

[12] Van der Corput, J. G. Zahlentheoretische Abschätzungen mit Anwending auf Gitterpunktprobleme. II. *Math. Zschr.*, 1928, т. XX VIII.

[13] Titchmarsh, E. G., *The zeta-function of Riemann*. Cambridge, University press, 1930.

[14] Brun. V., Über das Goldbachsche Gesetz und die Anzahl der Primzahlpaare. *Archiv for Mathematik og Naturvidenskab*, 1915, т. 34. H. 2, № 8.

[15] Hua Loo-Keng, Some Results in the Additive Prime-Number Theory. *Quart Journ. Math., Oxford Ser.*, 1938, т. 9.

[16] Шнирельман, Л. Г., Об аддитивных свойствах чисел. *Изв. донск. политехн. ин-та*, 1930, т. 14.

[17] Page, A., On the number of primes in an arithmetic progression. *Proc. London Math. Soc.*, II. S., 1935, т. 39.

[18] Estermann, T., Proof that every large integer is the sum of two primes and a square. *Proc. London Math. Soc.* II. S., 1937, т. 42.

(越民義譯)

譯 者 贅 言

本書譯自 И. М. 維諾格拉朵夫選集第 237—331 頁. 在選集出版之前,本書曾在 1947 年以單行本印出行世,列爲蘇聯科學院 Стеклов 數學研究所專刊第 23 集. 在 1937 年,著者曾寫了一本名爲“解析數論中的新方法”的書,所包括的方面與本書大致相同,也可以說是本書的前身. 但在處理問題的方法上及所得的結果上,本書又進了一步.

書裏系統地敍述了著者自己關於三角和數估值的新方法和它的應用. 閱讀本書,可以不必需要很多的知識. 若讀者對於(例如)華羅庚教授所著“數論導引”(不

久卽可出版)前面六章已有相當了解,卽可進行閱讀;書裏個別的地方,如第一章引理17 的證明,可參考華羅庚教授所著"堆壘素數論"第二章;第十章引理 1 (Page 定理)的證明,數學研究所數論組將有資料在本刊發表,讀者中若有無法覓得該引理之證明者,不妨暫時掠過. 書裏的結果在目前來說皆是最突出的. 若讀者欲明瞭與本書所論直接有關問題的發展,可參考上述的"堆壘素數論". 實際上,這兩本書也就包括了近代堆壘數論的主要內容.具有大學專業知識的讀者可通過它們進入這一領域的最前線. 這就是譯者翻譯本書的原因.

書裏涉及到堆壘數論中的兩個著名問題,卽哥特巴赫問題與華林問題.

哥特巴赫問題是哥特巴赫 (Гольбах) 在 1742 年致歐拉 (Euler) 的信中所提出的問題.他的問題是:每一大於 2 的偶數皆是兩個素數之和. 許許多多的事例(比如有人曾經把一百萬以內的數目皆加以計算)皆證明哥特巴赫的猜測成立. 然而直到本世紀初,對於這問題的具體貢獻還是沒有. 在 1912 年,蘭道 (Landau) 在英國劍橋國際數學會議上還曾說過:"哥特巴赫問題不是用現今的數學方法所能解決的".雖然如此,但近二十餘年來,這問題却得到了很大的進展.

首先對哥特巴赫問題直接作出重要貢獻的,是蘇聯學者史尼列爾曼 (Шнирельман). 他引進了一種叫做密率的觀念(參看上述"數論導引"),證明了 (1930) 所有充分大的整數皆是有限定多個素數之和. 史尼列爾曼的結果和方法立刻受到了很大的注意. 在 1935 年,羅曼諾夫 (Романов) 曾據原來的方法算出所有充分大的整數皆是不多於 2208 個素數之和. 其後又有人將 2208 逐步改爲 71, 67 (最近 (1950) 還有人將 67 減低到 20).

在另一方面對哥特巴赫問題作出重要貢獻的,是哈代與李托伍德 (Hardy 與 Littlewood). 在 1922 年,利用他們所創造的"圓法" (Circle method),這兩位學者證明了每一充分大的奇數皆是三個素數之和,並求出了表示方法的個數的漸近公式.但他們的結果却依賴於一個叫做"廣義黎曼假設"的眞實性,而這個假設到今天還是無法證明. 儘管他們的結果是奠基於一個未經證明的假設上,然而他們所用的方法在後來却發生了很大的影響.

對哥特巴赫問題作出了決定性的貢獻的,是維諾格拉朵夫. 他在 1937 年證明了每一充分大的奇數皆是三個素數之和,因而每一充分大的整數皆是四個素數之和.他的證明就是本書第九章及第十章的內容. 證明裏不再依賴任何的假設.

哥特巴赫問題後來又得到了許多的推廣和演變. 例如華羅庚教授曾證明每一充

分大的奇數皆是兩個素數與一個素數的 k（k 固定）次方之和；林尼克（Линник）曾證明每一充分大的整數皆是兩個素數和既定多個 2（或別的 >2 的整數）的乘冪之和;萊尼（Renyi）曾證明每一充分大的整數皆是一個素數與由有限定多個素數相乘所得之積之和,等等. 其主要的演變,後面我們將要談到.

我們要注意,儘管許多卓越的數學家在這問題上曾經作了很多的努力,並作出了巨大的貢獻,然而在現刻離哥特巴赫問題的完全解決仍有距離. 一方面是哥特巴赫原來所提出的問題:每一大於 4 的偶數皆是兩個素數之和,還未得到解決. 假如這一猜測得到證實,則奇數情形的哥特巴赫問題立刻可以推出；另一方面，維諾格拉朵夫的結果是指充分大的奇數而言. 也就是說所討論的數目必須要大於某一常數 c. 有人曾經算出此

$$c \leqslant e^{e^{e^{41.96}}},$$

而我們現在還無法將小於

$$e^{e^{e^{41.96}}}.$$

的一切奇數逐一加以驗算證明哥特巴赫的猜測成立.

華林問題是 1770 年華林（Waring）所提出的. 他的問題是：對於每一整數 $n \geqslant 2$，必存在一僅與 n 有關的數 $r = r(n)$，使得每一正整數皆可表為 r 個非負整數的 n 次方之和. 由這問題,直接即引起了下面的三個問題:

1. 這樣的 $r(n)$ 是否存在,若存在,則其最低的數目(記作 $g(n)$) 等於多少?
2. 若我們在問題裏所提的不是對"每一正整數"而言,而是對"每一充分大的整數"而言,我們即得一與 $g(n)$ 相應的數 $G(n)$，問 $G(n)$ 的最小上界是多少?
3. 若充分大的正整數 N 已經給定,則將 N 表成 r 個非負整數的 n 次方之和的方法的種數 $I(N)$，當 N 無限增大時,其主項為何?

首先解決華林所提出的問題的,是希爾柏特（Hilbert）. 他的結果是在 1909 年發表的. 他證明確有一 $t(n)$ 存在，使得所有的正整數皆可表為 $t(n)$ 個非負整數的 n 次方之和. 但希爾柏特所得出來的 $t(n)$ 太大,方法也很特殊，後來雖經許多人加以改進,但收效還是不大.

繼希爾柏特之後,在華林問題上作出重要貢獻的是哈代與李托伍德. 這兩位學者以他們自已所創造的"圓法"來研究華林問題. 他們證明當 $r \geqslant (n-2)2^{n-1}+5$，$(n>2)$ 時,有漸近公式

$$I(N)=\frac{\left(\Gamma\left(1+\frac{1}{n}\right)\right)^r}{\Gamma\left(\frac{r}{n}\right)}N^{\frac{r}{n}-1}\mathfrak{S}+O\left(N^{\frac{r}{n}-1-c}\right), \tag{1}$$

這裏的 $c=c(n)$ 是一正常數，$\mathfrak{S}$ 爲奇異級數(見本書第二章)．

對於華林問題貢獻最大的是維諾格拉朵夫． 他最初關於華林問題的論文是在 1924 年發表的． 在 1934 年，他引入了一種新的觀念，大大地改進了前人對於華林問題所得的結果． 他對於華林問題的研究持續了很多年，逐次得出了許多光輝的結果(詳見下面的表)． 本書中已將 (1) 式成立所需的 $r(n)$ 降至 $r(n)\leqslant[10n^2\log n]$ $(n\geqslant 12)$． 華羅庚教授在 1947 年又將此 $r(n)$ 降至 $r(n)\leqslant 2n^2(2\log n+\log\log n+$ $+2.5)$．

對於數學家最感興趣的是關於 $G(n)$ 的研究． 有人曾經做過許多的數字計算，看出數目越大，所需要用來表示它的項數就越少． 比如說，只有 23 一數需要 9 個立方數來表示，其餘小於 455 的數至多需要 8 個立方數來表示，而從 455 到 12000 之間的數則至多只需要 7 個立方數來表示等等． 因此，假若需要項數最多的只是極其少數的幾個數，我們就不應該把研究的結果限制在這幾個數上面． 哈代與李托伍德曾證明

$$G(m)\leqslant\left(\frac{n}{2}-1\right)2^{n-1}+n+5+\left[\frac{(n-2)\log 2-\log n+\log(n-2)}{\log n-\log(n-1)}\right].$$

維諾格拉朵夫用他自己的方法將哈代與李托伍德的結果大爲改進，在華林問題上作出了巨大的貢獻． 我們現將他在 1934—1938 年間在這問題上所得到的結果列表如下(由於手邊資料的缺乏，難免有所遺漏)：

年　代	$G(n)\leqslant$	$r(n)\leqslant$
1934	$32n^2(\log n)^2$	
1935	$2[n(n-2)\log n+2n]$	
1935	$n(6\log n+\log 216+4)$	$183n^9(1+\log n)^2$
1935		$91n^8(\log n+1)^2$
1936		$131n^5(\log n)^2$

1936		$10n^3\log n$
1937		$\left(1+2.2\frac{\log\log n}{\log n}\right)n^3\log n$
1938	$n(4\log n+8\log\log n+12)$	

本書中又改進到 $G(n)\leqslant n(3\log n+11)$. 不難證明 $G(n)>n$，因此維諾格拉朵夫的結果與最終的結果至多只差一 $\log n$ 的階.

由上所述，我們可以看出維諾格拉朵夫在數論上的輝煌成就乃是他數十年如一日的不斷辛勤勞動的結果. 蘇聯最高蘇維埃主席團在 1945 年曾授予他以社會主義勞動英雄的光榮稱號.

維諾格拉朵夫的方法還可以利用來決定 $g(n)$. 大約在 1772 年,歐拉曾經推斷 $g(n)=2^n+\left[\left(\frac{3}{2}\right)^n\right]-2$. 在 1936 年，狄克遜 (Dickson) 及皮賴 (Pillai) 即依據維諾格拉朵夫的方法及"遞升法" (method of ascent) 證明當 $n>6$ 時,除了某些特殊的 n 之外,歐拉的猜測皆成立. 其後 (1944)，尼文 (Niven) 證明歐拉的猜測對於這些特殊的 n 也成立. 現刻尚未解決的僅是 $n=4$, 5 兩種情形. 對於這兩種情形,目前最好的結果是:

$$19\leqslant g(4)\leqslant 35;\ 37\leqslant g(5)\leqslant 54.$$

由華林問題及哥特巴赫問題，我們可以聯想到是否存在一僅與 n 有關的數目 $r(n)$，使不定方程

$$N=p_1^n+\cdots+p_s^n$$

對於任何 N 及 $s\geqslant r(n)$ 可解,這裏的 p_i $(i=1,\cdots,s)$ 是限取素數或 0. 這兒又建議我們下面的問題: 决定 $r(n)$，使不定方程組

$$p_1^n+\cdots+p_s^n=N_n,$$
$$\cdots\cdots\cdots\cdots$$
$$p_1+\cdots+p_s=N_1$$

當 $s\geqslant r(n)$ 時對任何 $N_1,\cdots,N_n$ 可解. 問題自然還可以更加推廣. 對於更詳細的介紹問題，誠如維諾格拉朵夫在本書敍言中所說，"我們介紹讀者去看華羅庚的優秀專著".

維諾格拉朵夫的方法除用於上述兩個問題及本書中第五章及第十章所述用於整

多項式値的分數部份之分佈問題之外，還有着許多別的重要應用. 華羅庚教授在他的"堆疊素數論"第一版的附錄中，當證明一條關於三角和數

$$\sum_{x=Q+1}^{Q+P} e^{2\pi i f(x)}$$

的估値的引理之後，曾有這樣的一段話:

"這一引理在解析數論、黎曼 ζ- 函數論等等之內，有着重要的意義. 我們現來敍述它的幾個應用，這些應用可以從已知的方法(下面公式右角上的數字卽表示有關所述方法的參考文獻——譯者)無須重大改變卽可證明:

1) $\zeta(1+it)=O((\log t)^{3/4+\varepsilon})$[1];

2) $\pi(x)=\mathrm{li}\,x+O(x\,e^{-A(\log x)^{4/7-\varepsilon}})$[2];

3) 中値公式

$$\lim_{T\to\infty}\frac{1}{T}\int_0^T|\zeta(\sigma+it)|^{2k}dt=\sum_{n=1}^{\infty}d_k^2(n)\,n^{-2\sigma}$$ [3]

之有效區域;

4) 設 $A(x)$ 爲橢體

$$\sum_{i,j=1}^{4}a_{ij}x_ix_j\leqslant x\quad(a_{ij}=a_{ji}\ \text{爲整數})$$

內的整點數，D 爲此二次形式之行列式. 則

$$A(x)-\frac{\pi^2}{2\sqrt{D}}x^2=O(x(\log x)^{3/4+\varepsilon})$$ [4]".

維諾格拉朵夫的方法又可利用來决定一定包含素數的區間之長. 邱達可夫(Чудаков)在 1936 年曾由此證明當 N 甚大時，區間 $(N, N+AN^{\frac{3}{4}+\varepsilon})$ 內必有素數，此處的 A 爲一絕對常數. (1937 年 Ingham 曾將 $\frac{3}{4}$ 改進爲 $\frac{5}{8}$); 也可以用來證明不定方程

$$p_1+p_2-p_3=1$$

有無窮多解等等.

1. Titchmarsh, *Quarterly Journ. of Math.*, **9** (1938), 97—107.
2. Чудаков, *ДАН СССР*, XXI (1938), 421—422, 又 Titchmarsh 1.
3. Davenport, *Journ. of London Math. Soc.*, **10** (1935), 136—138.
4. Walfisz, *Travaux de l'Institut Mathématique de Tbilici*, **5** (1938), 181—196.